# 一种可伸缩性视频加密方案

梅竞晋 张 荣 胡 洋
(中国科学技术大学电子工程与信息科学系多媒体计算与通信教育部-微软重点实验室, 合肥 230027)

**摘 要** 随着网络的不断普及和发展,数字视频在网络中有了越来越多的应用,随之也提出了视频安全性问题,通过视频加密可以很好地解决此问题。为了满足网络对视频加密的要求,设计了一种可伸缩性视频加密的方案。考虑到小波的多尺度性,建立了一个基于小波变换的视频压缩平台,在此平台上进行了仿真加密实验,即在压缩的过程中从小波系数置乱、系数随机翻牌、运动矢量置乱等方面进行加密,并与其他算法进行了比较实验。实验结果表明,该方案具有加密效果好,密钥量较低,安全性好等优点,同时对压缩比和压缩效率有较好的保持,是一种高效的视频加密方案。

**关键词** 视频加密 小波系数 运动矢量
**中图法分类号**: TN919.81 **文献标识码**: A **文章编号**: 1006-8961(2006)10-1400-05

# A Scalable Encryption Scheme for Video

MEI Jing-jin, ZHANG Rong, HU Yang
(*Department of Electronic and Engineering and Information Science, MOE-Microsoft Key Laboratory of Multimedia Computing and Communication, University of Science and Technology of China, Hefei* 230027)

**Abstract** With the development of network, video has been widely used in it, and the security problem of video has been brought forward. We can solve the problem with video encryption. According to the requirement of network to video encryption, this paper proposed a new scalable encryption scheme. This paper set up a video compression system based on wavelet transform, encrypt on wavelet coefficients and motion vectors shuffling, sigh flipping in the encoder, and also compared the experimental results with other schemes. Those results show this scheme can get better encryption effect, be of less key cost and higher security. At the same time, it also has small impact on compression efficiency and compression ratio. It is a high efficiency scheme of video encryption.

**Keywords** video encryption, wavelet coefficient, motion vector

## 1 引 言

随着网络技术的不断发展,视频在越来越多的领域取得了应用,随之而来的是如何使视频更加符合网络要求,在网络上得到更好的传输。尤其是在许多特殊的领域(数字电视,视频会议,机密文件传输等)需要对视频进行保护,即视频加密。如何进行视频加密,如何达到最好的加密效果,如何使加密结果更适合在网络中传输等等,都已经成为了当前的热点问题。

视频是由许多帧连续的图像组成,具有编码结构特殊、数据量大、通常采用压缩格式传输等特点[1]。视频加密就是通过密钥与图像中的某些特定参数进行某种设定的操作后从而改变图像数据的排列,使人们无法在未经解密的情况下获得正确解码的视频。它所实现的功能就是对视频码流的排列进行改变。由于没有解密就无法获得正确解码的视频,换言之就是无法看到未经授权的视频,从而保证了所需要的数字视频保密,从而确保了安全。而传

**收稿日期**:2004-12-20;**改回日期**:2005-09-09

**第一作者简介**:梅竞晋(1980~ ),男。中国科学技术大学电子工程与信息科学系硕士研究生。主要研究方向为视频压缩、视频加密。E-mail: meijj@mail.ustc.edu.cn

统的数据加密算法如果直接使用,很难满足视频的实时性要求,因此一般考虑在压缩的过程中进行加密。这类加密算法由于充分考虑了视频编码的过程,在实现加密的同时也保证了一定的压缩性能,因此一般具有实时性较好,压缩质量高等优点。目前视频加密的方案有两大类:

(1)基于 DCT 的加密　主要是针对各种视频压缩标准,如 H.263,H.264,MPEG-1,2,4 等等,通过对变换系数的置乱,进行选择性加密[2,3],如 MPEG 视频流的高效多层编码和加密[4];VEA1 算法[5]等等。

(2)基于 DWT 的加密　由于小波变换的多尺度特性,使得码流具有可伸缩性,符合网络对视频流的要求,保证了视频可让各种不同带宽的用户使用。因此,在基于小波变换的视频压缩框架下进行加密,可以满足网络对视频流的可伸缩性要求,如文献[6]中已经提到的 3 种通过置乱小波系数加密图像的方法,如图 1 所示。

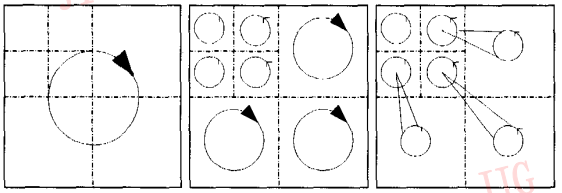



图 1　3 种小波系数置乱方法

Fig. 1　Three kind of confusion methods of wavelet coefficients

第 1 种方法如图 1(a)所示,称为全局小波系数置乱(CWW),该方法是在视频中每帧图像范围内对小波系数进行置乱。该方法的优点是安全性好,缺点是密钥量大,且有高低频系数之间的迁移,对压缩效率影响极大,无法进行有损压缩图像的加密。

第 2 种方法如图 1(b)所示,称为同频子带小波系数置乱(CWF),该方法是在各个频带内对该频带范围内的小波系数进行置乱。该方法的优点是没有高低频系数之间的迁移,可以支持有损压缩图像的加密,缺点是密钥开销和计算量都较大。

第 3 种方法如图 1(c)所示,称为四叉树小波系数置乱(CWQ),该方法充分利用了编码的树型结构,即在低一级的子块中以相应 2×2 块为单位块,按较高一级子块规则置乱,同时在子块中再置乱。这种方法在保证了高低频系数独立的基础上,在密钥量降低、加密效果上都较第 2 种方法有了较大的提高,但它的缺点在于计算比较复杂,对压缩时间有较大的影响。

针对 DWT 的多尺度特性,提出了一套完整的可伸缩性加密方案,在原始视频的压缩编码过程中,通过加入对小波系数和运动矢量(MV)进行实时加密处理的模块,完成在视频压缩过程中同时加密的功能。具体又分为以下两部分:

(1) 处理 I 帧　对小波系数置乱和符号翻牌;

(2) 处理 P 帧　分别进行残差小波系数置乱、符号翻牌、MV 置乱、MV 符号翻牌。

通过实验证明此方案完全解决了原有所有方案密钥量大,无法满足一定的压缩率的缺点,在密钥量和计算量上均有大大降低,从而可以保证压缩加密时间,使其满足视频实时处理的要求;同时继承了 CWF 方案主观效果较好的优点,从实验结果可以知道加密效果完全符合要求,能够实现视频内容保密的目的。

## 2　加密流程

由于小波变换的多尺度特性能够很好地适应网络可伸缩性的需要,选择了基于 DWT 的压缩加密算法,这样就使本文加密方案具有可伸缩性。

具体的编码端流程如图 2 所示,输入视频按 I,P 帧分类分别处理。I 帧直接采用小波零树编码算法;P 帧则首先利用前一个视频帧进行基于块的运动估计和运动补偿,形成当前帧的预测帧,再将当前帧和预测帧相减得到的残差用小波零树编码算法进行编码。在小波变换后加入加密部分(图中灰色模块),为了保证预测帧的正确性,在量化后还要进行一次解密(图中灰色模块),然后对于

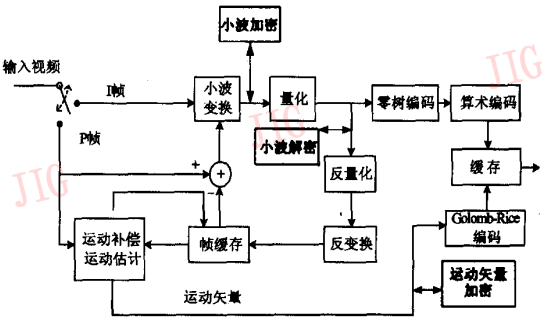



图 2　编码端流程

Fig. 2　Flow chart of encoder

运动矢量同时进行加密(图中灰色模块),这样就完成了视频的加密过程。同时将密钥用标准的加密算法(如 DES)加密后作为输出密钥。解码端与编码端过程相反,在正确的密钥基础上即可获得正确的视频解码。

## 3 加密算法

图 2 中小波加密模块和运动矢量加密模块是整个加密流程的核心。在小波加密模块中,具体进行了两个主要步骤:一是对小波系数进行置乱;二是对于小波系数进行符号随机翻牌。而在运动矢量机密模块中同样有以下两个主要步骤:一是对运动矢量进行置乱;二是对运动矢量进行符号随机翻牌。

### 3.1 小波加密模块

在小波加密模块中包括小波变换后的加密部分和获得预测帧之前的解密部分。加密部分包括了小波系数置乱和符号随机翻牌两个步骤,而解密部分则是加密的逆过程。

#### 3.1.1 小波系数加密算法

对小波系数进行加密的一个较好方法是对小波系数进行置乱。在文献[9]提出的 3 种置乱小波的方法基础上,提出了一种基于小波多尺度分解特性的算法。此算法中设置了 4 个置乱表,在对应子带中采用相应的分块置乱处理。从理论分析和实验结果证明,该方法具有安全性较高、计算复杂度低、密钥开销小、对压缩效率影响小的特点。

该算法的基本原理图如图 3 所示。

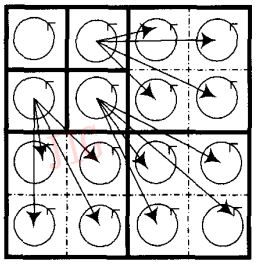


图 3 小波系数置乱方法

Fig. 3 The confusion method of wavelet coefficient

具体步骤如下:

(1) 对于 $M \times N(M = 2^m, N = 2^n)$ 的 I 帧和 P 帧残差进行 $L$ 级小波变换,变换后 $LL_0$ 小波边带的尺寸为 $I \times J$,其中:

$$I = 2^{m-L},\ J = 2^{n-L} \tag{1}$$

(2) 随机生成 4 个置乱表 $TLL_0$、$TLH_1$、$THL_1$ 和 $THH_1$,表的大小为 $I \times J$,对 $LL_0$、$LH_1$、$HL_1$ 和 $HH_1$ 边带分别用表 $TLL_0$、$TLH_1$、$THL_1$ 和 $THH_1$ 进行置乱;

(3) 对第 $k(1 < k < L)$ 个波段系数 $LH_k$、$HL_k$ 和 $HH_k$ 均分成 $I \times J$ 大小的小块,对 $LH_k$、$HL_k$ 和 $HH_k$ 边带以块为单位分别用 $TLH_1$、$THL_1$ 和 $THH_1$ 进行置乱。

下面就该算法的性能进行分析:

(1) 安全性

所处理的视频均为彩色图像(多通道的图像),按 YUV 对各通道分别置乱,将大大增加安全性。更重要的是,由于小波分解的特性,原始图像的能量分布在加密图像之中得以较好地隐藏,传统的基于能量分析的密图攻克法将失效,这将更加有利于图像加密。

(2) 密钥空间

对于一幅 $M \times N$ 的灰度图来说,假设小波分解的级数为 $L$,则该方法的密钥空间 $K_c$ 为

$$K_c(M,N,L) = \left[\frac{M \times N}{2^{2L}}!\right]^4 \tag{2}$$

当视频为 QCIF($M = 176, N = 144$)时,小波分解级数为 4($L = 4$),则 $K = 7.59 \times 10^{623}$。很显然此密钥空间足够保证视频加密的安全性,并没有因此而降低安全性。同时可以简单地看出此方法的密钥开销比其他 3 种算法小。

(3) 压缩效率

与方法 CWF,CWQ 一样,这种方法保证了系数只在同频带内被置乱,不会发生高低频系数之间的迁移,这样就保证了后面量化的时候对于很少系数为 0 的低频子带能分配较多的量化比特,而对于高频子带则分配较少的量化比特,很好地保证了编码效率。

#### 3.1.2 符号加密(随机翻牌)(Sign Encryption, SE)

除了系数置乱之外,还采用符号加密的方法来进一步加强安全性。符号加密是通过由 0、1 比特位组成的密钥序列和小波系数符号位进行异或,从而达到很大程度改变原视频的目的[9]。

考虑到计算复杂度和密钥开销的问题,不采用对每个符号进行加密,而选用块符号加密的方法。具体方法是先将整幅图按上面的分块方式进行分块,再以块为单位进行符号变换。即以密钥序列的一个 0、1 比特位和对应块的每个系数的符号位进行异或。这样做的主要好处是可以极大减少计算复杂

度和密钥开销,而且实验结果表明主观加密效果与全局符号加密方法相近。

块符号加密的安全性低于全局符号加密。假设块大小取 $I \times J$,由此产生的密钥空间 $K_{SE}$ 为

$$K_{SE}(N,M,I,J) = 2^{\frac{MN}{IJ}} \tag{3}$$

视频为 QCIF,块的大小为 11 ×9 时,密钥空间 $K_{SE} = 1.16 \times 10^{77}$。

对于符号加密来说,虽然完全破译难度很大,但由于符号加密仅仅改变了符号位的信息,因此必须与前面所用的小波置乱方法结合,才能起到进一步增加安全性的目的。此时总的密钥空间将变为

$$K_{CSE} = K_C \times K_{SE} \tag{4}$$

其中,$K_C$ 为小波置乱的密钥空间,$K_{SE}$ 为符号加密的密钥空间。

### 3.2　运动矢量(MV)加密模块

由于对 P 帧是对残差进行小波加密的,这样每帧加密的图像单独看效果很好,可是如果把视频连续播放,就会发现视频中物体的运动轨迹还是可见的,因此还需要对运动矢量(MV)进行加密。在运动矢量加密模块中,同样有运动矢量置乱和符号随机翻牌两个步骤。

#### 3.2.1　运动矢量加密算法

对于运动矢量加密,还是采用类似小波系数的置乱方法,只是这里要分别考虑编码过程中图像分块的大小,由这个大小决定置乱系数的设置。

具体的运动矢量加密算法为对于每个分块的运动矢量,首先判断块的大小;然后建立对应大小的置乱表,这里由于编码中只有 4 ×4,4 ×8,8 ×4,8 ×8 4 种分块,所以建立 4 个置乱表即可;最后根据对应的置乱表对运动矢量进行置乱。

由于加密的是视频,所以在只对每帧加密后是不能够满足安全性要求的。在对运动矢量进行加密后,有效地去除了帧与帧之间的联系,对于加密效果有着相当大的提高,同时很好地满足了安全性的要求了。

对于上述加密的密钥开销,可以知道所需的密钥量仅为相当小的一部分,相对于小波系数加密的密钥开销而言,运动矢量加密的密钥开销几乎可以忽略。

#### 3.2.2　符号加密(随机翻牌)(Sign Encryption,SE)

同小波系数加密一样,在对运动矢量进行置乱以后同样进行符号加密,即符号随机翻牌。同样仍然采用对应于块的符号翻牌,这样即可以节省密钥开销,也可以使加密效果得到进一步的增强。

## 4　实验结果

根据图 2 所示的框架,搭建一个基于 DWT 的压缩验证平台,该平台与 H.264 标准在压缩效率、压缩比等参数上均相当,如表 1 所示。

**表 1　压缩平台与 H.264 性能比较**

**Tab.1　Comparison of ours and H.264**

| 视频 | 比特(K) | Y/C | SNR | |
|---|---|---|---|---|
| | | | H.264 | 本文算法 |
| Akiyo | 14 | Y | 34.29 | 34.21 |
| | | C | 38.75 | 38.50 |
| Akiyo | 28 | Y | 40.99 | 40.21 |
| | | C | 43.47 | 42.36 |
| News | 14 | Y | 30.17 | 30.13 |
| | | C | 35.49 | 35.00 |
| News | 27 | Y | 35.56 | 35.37 |
| | | C | 39.55 | 37.48 |

在这个平台上加入本文的加密方案,并与 CWW、CWF、CWQ 等算法进行比较,表 2 是 football 标准序列的测试结果。

对压缩时间的影响是指加密过程占整个编码过程时间百分比;对压缩率的影响是指密钥占原文件大小的百分比。

**表 2　不同小波置乱方法的性能比较**

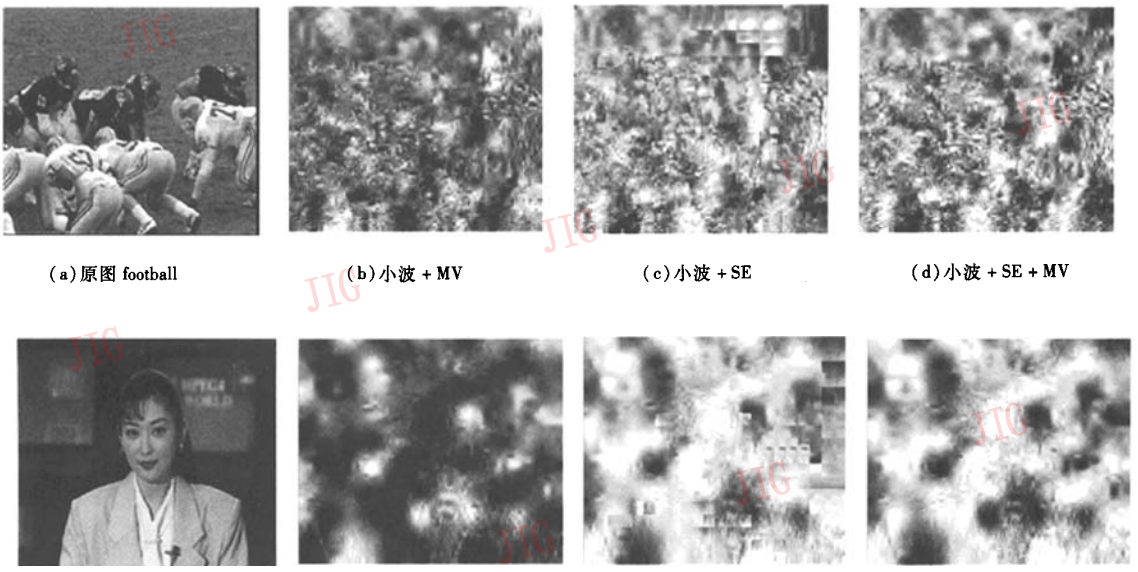
**Tab.2　Comparison of four encryption scheme**

单位:%

| | CWW | CWF | CWQ | 本文算法 |
|---|---|---|---|---|
| 对压缩时间的影响 | 14 | 13 | 4 | 1 |
| 对压缩率的影响 | 0.8 | 0.2 | 0.15 | 0.07 |

实验结果表明,本文算法要优于 CWF 和 CWQ 算法。另外,本文算法和无加密时的压缩比相比,差别是非常小的,这充分证明本文算法完全适用于有损压缩。

为了对加密的主观效果进行验证,实验选用标准序列 football 和 Akiyo 对本文算法进行了实验。如图 4 所示。实验结果表明,本文算法能较好地满足对加密效果的要求。



(a)原图 football (b)小波 + MV (c)小波 + SE (d)小波 + SE + MV

(e)原图 Akiyo (f)小波 + MV (g)小波 + SE (h)小波 + SE + MV

图 4 加密效果图

Fig. 4 Results of encryption

## 5 结 论

本文提出了一种可伸缩性的视频加密方案,通过在基于 DWT 编码过程中对小波系数和运动矢量置乱,并结合符号翻牌,以达到视频数据保密的目的。通过理论分析和实验结果证明本方法具有安全性好、加密效果好、对压缩性能影响小的特点,适用于实时处理,满足可伸缩性要求,具有良好的应用前景。同时为了达到更好的压缩效果、压缩比和时间可伸缩性,还可以通过 3 维小波变换来完成编码,这将是下一步的工作重点。

## 参考文献(References)


1 Kuo C J. Novel, image encryption technique and its application in progress transmission [J]. Journal of Electronic Imaging, 1993, 2(4):345 ~ 351.

2 Gan Xiao-ying, Sun Shi-ying, Song Wen-tao. A new encrypt ion algorithm for digital video based on pseudo-random sequence [J]. Journal of Data Acquisition & Processing, 2002, 17(3):284 ~ 151. [甘小莺,孙诗瑛,宋文涛. 基于伪随机序列的视频图象加密新算法[J]. 数据采集与处理, 2002, 17(3):284 ~ 151.]

3 LIAN Shi-guo, SUN Jin-sheng, Wang Zhi-quan. Quality analysis of several typical MPEG video encryption algorithms [J]. Journal of Image and Graphics, 2004, 9(4):483 ~ 490. [廉士国,孙金生,王执铨. 几种典型视频加密算法的性能评价[J]. 中国图象图形学报, 2004, 9(4):483 ~ 490.]

4 Tosun A S, Feng W C. Efficient multi-layer coding and encryption of MPEG video streams [A]. In: 2000 IEEE International Conference on Multimedia Computing and Systems [C], New York City, NY, USA, 2000:119 ~ 122.

5 Qiao L, Nahrstedt K. A new algorithm for mpeg video encryption [A]. In: Proceedings of the First International Conference on Imaging Science, Systems, and Technology (CISST' 97) [C], Las Vegas, Nevada, USA, 1997: 21 ~ 29.

6 Lian Shi-guo, Wang Zhi-quan. Comparison of several wavelet coefficient confusion methods applied in multimedia encryption [A]. In: Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC' 03) [C], Shanghai, China, 2003: 372 ~ 376.

7 Maniccam, Suchindran, Sanmuganathan. Image-video Compression, Encryption, and Information Hiding [D], Binghaminton, New York, USA: State University of New York, 2001.

8 Lei Tang. Methods for encrypting and decrypting MPEG video data efficiently [A]. In: Proceedings ACM Multimedia96 [C], Boston, MA, USA, 1996: 219 ~ 229.

9 Zeng Wen-jun, Lei Shawmin. Efficient frequency domain video scrambling for content access control [A]. In: Proceedings of the Seventh ACM International Conference on Multimedia (Part 1) [C], Orlando, FL, USA, 1999: 285 ~ 294.

10 Wen Jiang-tao, Severa M, Zeng Wen-jun, *et al*. A format-compliant configurable encryption framework for access control of multimedia [A]. In: 2001 IEEE Fourth Workshop on Multimedia Signal Processing [C], Cannes, France, 2001:435 ~ 440.