US 20070248226A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2007/0248226 A1**

Chong et al. (43) **Pub. Date: Oct. 25, 2007**

(54) **SYSTEM AND METHOD FOR FAST AND SCALABLE MULTIMEDIA AUTHENTICATION IN REAL TIME ENVIRONMENT**

(75) Inventors: **Chan Fung Chong**, Hong Kong (CN); **Kam Pui Chow**, Hong Kong (CN); **Hing Yip Chung**, Hong Kong (CN); **Chi Kwong Hui**, Hong Kong (CN); **Kin Ying Yu**, Hong Kong (CN); **Ka Ying Lai**, Hong Kong (CN); **Fuk Sang Mak**, Kowloon (CN); **Shiu Hang Kenneth Tsang**, Kowloon (CN)

Correspondence Address:
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404 (US)

(73) Assignees: **THE UNIVERSITY OF HONG KONG**, Hong Kong (CN); **MULTIVISION INTELLIGENT SURVEILLANCE (HK) LTD.**, Hong Kong (CN)

(21) Appl. No.: **11/410,004**

(22) Filed: **Apr. 25, 2006**

Publication Classification

(51) **Int. Cl.**
H04N 7/167 (2006.01)

(52) **U.S. Cl.** **380/200**

(57) **ABSTRACT**

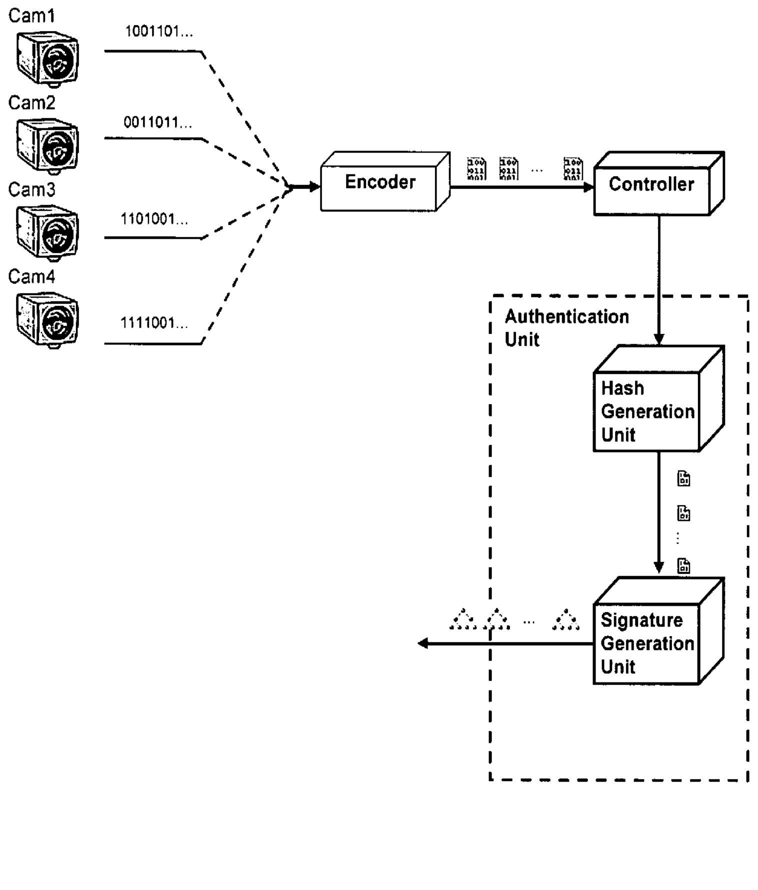
A method of processing a plurality of digital data files including at least one group of medium data files for constituting a sequence of events or activities of a time interval for secure delivery of the digital data files, the method comprising the steps of:

(a) processing a plurality of digital data files so as to generate a file identification value for each digital data file, wherein the file identification value of a digital data file is an one-way arithmetic value characteristic of the data content of the digital data file;

(b) processing the file identification values to generate an authentication root value, the authentication root value being an one-way arithmetic value characteristic of the plurality of file identification values;

(c) encrypting the root value; and

(d) grouping the encrypted authentication root value and a selected plurality of digital data files with a set of authentication information for delivery, wherein the set of authentication information is derived from the file identification values and is for deriving a test root value when in combination with said selected plurality of digital data files, and wherein the test root value is for comparison with the authentication root value to detect tampering of said selected plurality of data files.



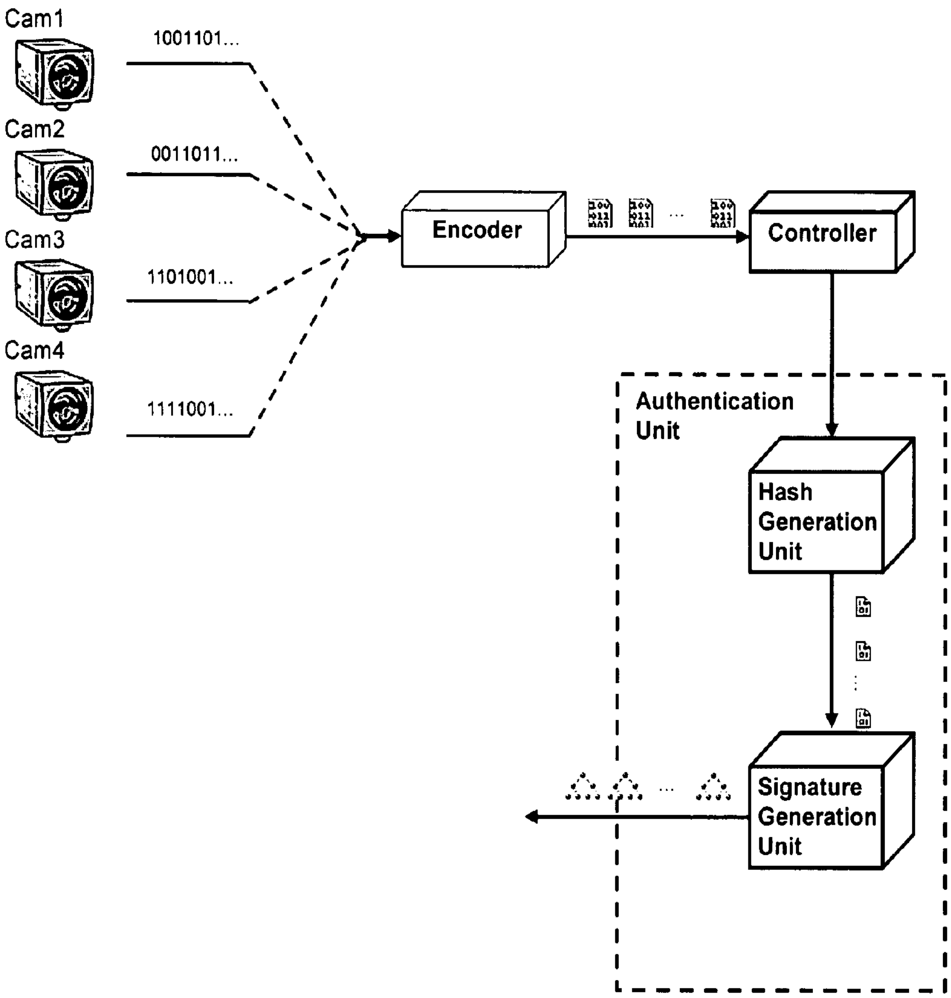

Cam1
1001101...
Cam2
0011011...
Cam3
1101001...
Cam4
1111001...
Encoder
Controller
Authentication Unit
Hash Generation Unit
Signature Generation Unit

Fig. 1

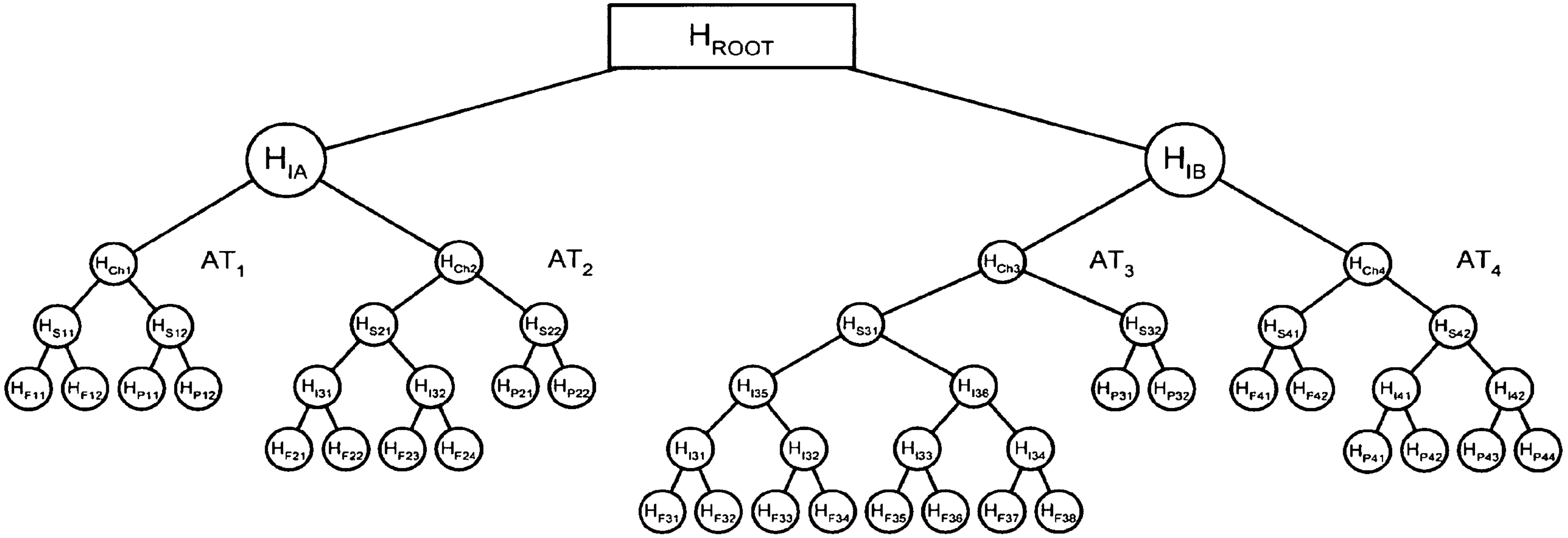

H_{ROOT}
H_{IA}
H_{IB}
H_{Ch1}
AT_1
H_{Ch2}
AT_2
H_{Ch3}
AT_3
H_{Ch4}
AT_4
H_{S11}
H_{S12}
H_{S21}
H_{S22}
H_{S31}
H_{S32}
H_{S41}
H_{S42}
H_{F11}
H_{F12}
H_{P11}
H_{P12}
H_{I31}
H_{I32}
H_{P21}
H_{P22}
H_{I35}
H_{I36}
H_{P31}
H_{P32}
H_{F41}
H_{F42}
H_{I41}
H_{I42}
H_{F21}
H_{F22}
H_{F23}
H_{F24}
H_{I31}
H_{I32}
H_{I33}
H_{I34}
H_{P41}
H_{P42}
H_{P43}
H_{P44}
H_{F31}
H_{F32}
H_{F33}
H_{F34}
H_{F35}
H_{F36}
H_{F37}
H_{F38}

Fig. 2

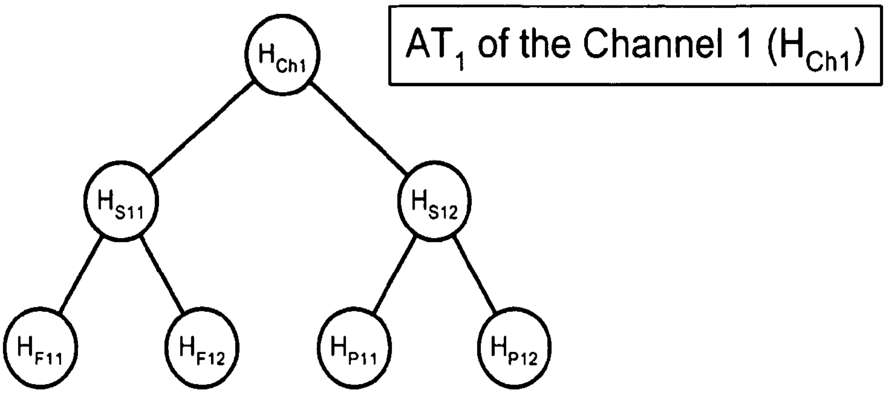

AT$_1$ of the Channel 1 (H$_{Ch1}$)
H$_{Ch1}$
H$_{S11}$
H$_{S12}$
H$_{F11}$
H$_{F12}$
H$_{P11}$
H$_{P12}$

Fig. 3a

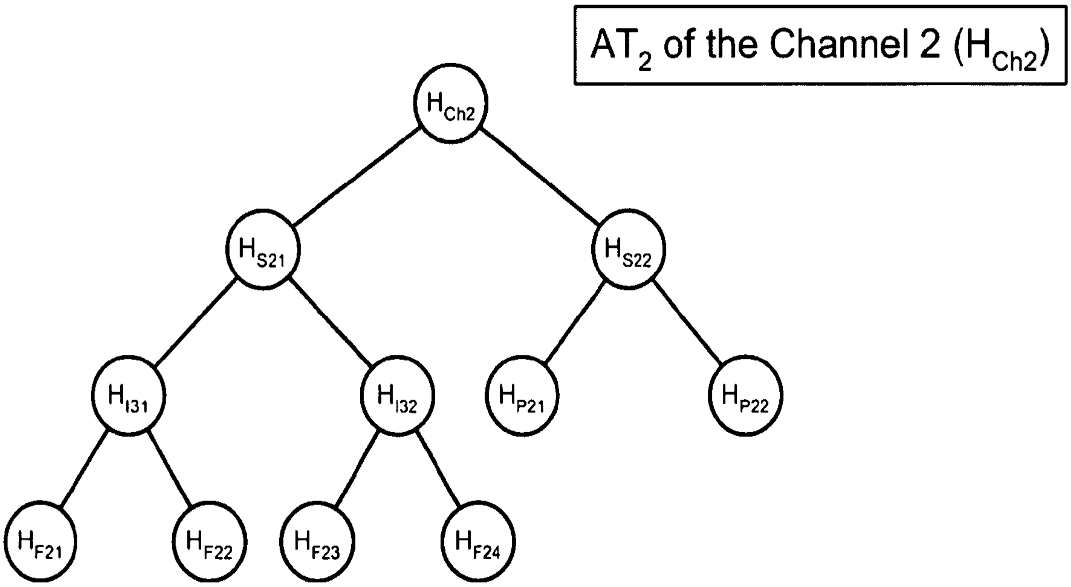

AT$_2$ of the Channel 2 (H$_{Ch2}$)
H$_{Ch2}$
H$_{S21}$
H$_{S22}$
H$_{I31}$
H$_{I32}$
H$_{P21}$
H$_{P22}$
H$_{F21}$
H$_{F22}$
H$_{F23}$
H$_{F24}$

Fig. 3b

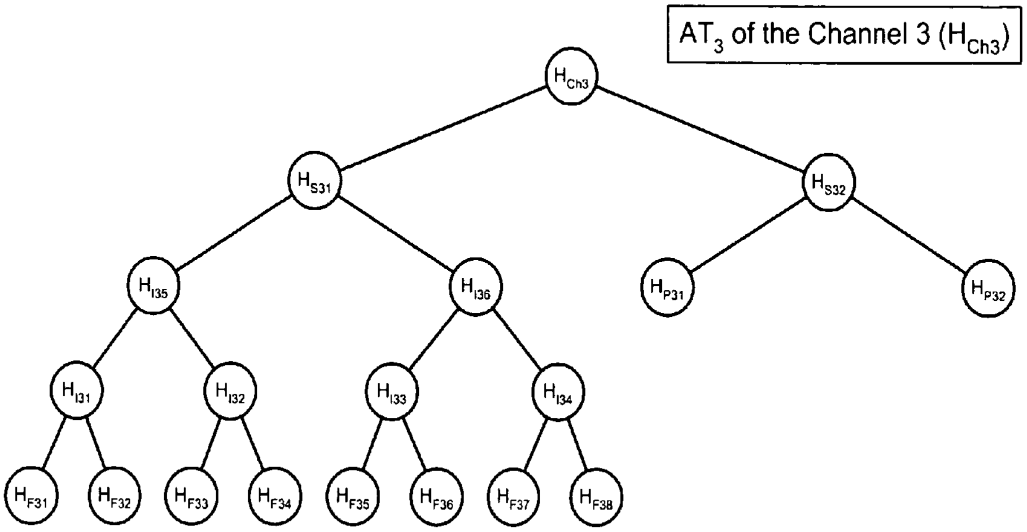

AT_3 of the Channel 3 (H_{Ch3})
H_{Ch3}
H_{S31}
H_{S32}
H_{I35}
H_{I36}
H_{P31}
H_{P32}
H_{I31}
H_{I32}
H_{I33}
H_{I34}
H_{F31}
H_{F32}
H_{F33}
H_{F34}
H_{F35}
H_{F36}
H_{F37}
H_{F38}

Fig.3c

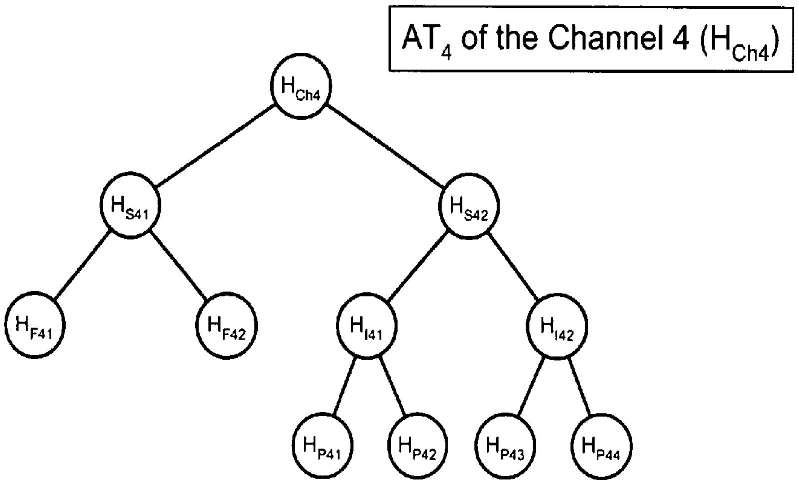

AT_4 of the Channel 4 (H_{Ch4})
H_{Ch4}
H_{S41}
H_{S42}
H_{F41}
H_{F42}
H_{I41}
H_{I42}
H_{P41}
H_{P42}
H_{P43}
H_{P44}

Fig. 3d

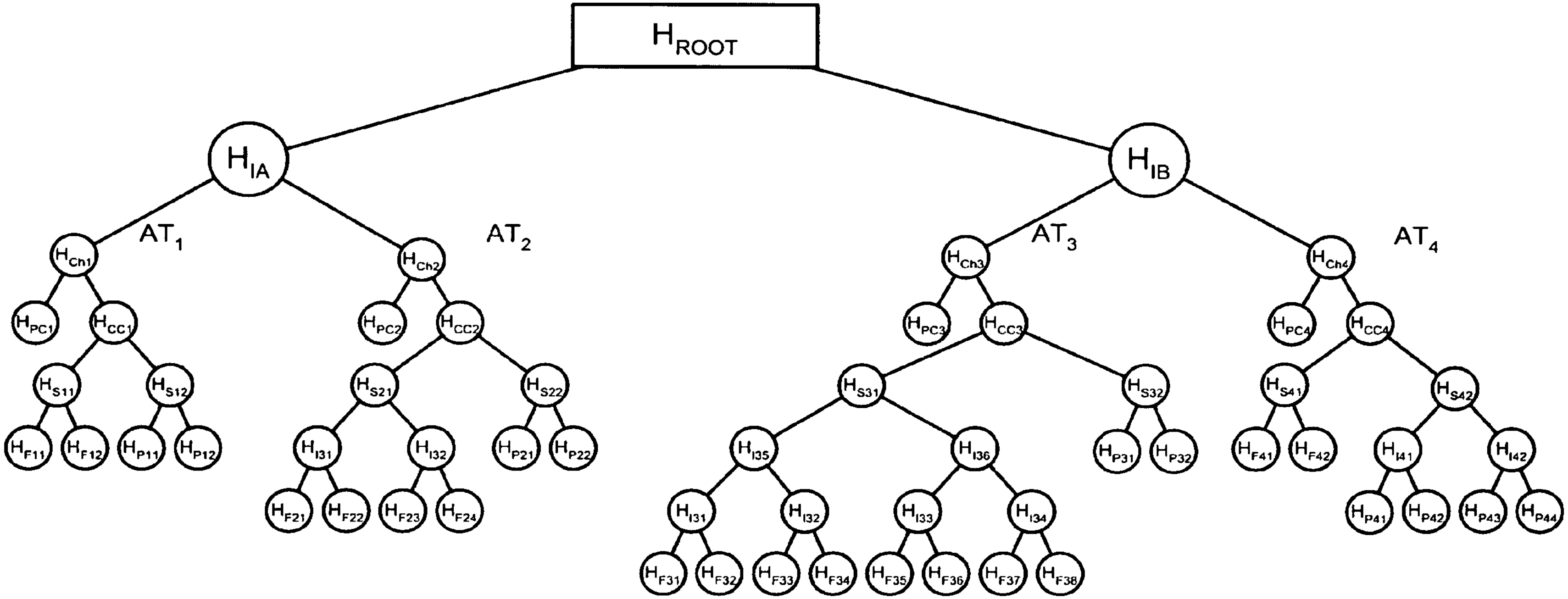

H_{ROOT}
H_{IA}
H_{IB}
AT_1
AT_2
AT_3
AT_4
H_{Ch1}
H_{Ch2}
H_{Ch3}
H_{Ch4}
H_{PC1}
H_{CC1}
H_{PC2}
H_{CC2}
H_{PC3}
H_{CC3}
H_{PC4}
H_{CC4}
H_{S11}
H_{S12}
H_{S21}
H_{S22}
H_{S31}
H_{S32}
H_{S41}
H_{S42}
H_{F11}
H_{F12}
H_{P11}
H_{P12}
H_{I31}
H_{I32}
H_{P21}
H_{P22}
H_{I35}
H_{I36}
H_{P31}
H_{P32}
H_{F41}
H_{F42}
H_{I41}
H_{I42}
H_{F21}
H_{F22}
H_{F23}
H_{F24}
H_{I31}
H_{I32}
H_{I33}
H_{I34}
H_{P41}
H_{P42}
H_{P43}
H_{P44}
H_{F31}
H_{F32}
H_{F33}
H_{F34}
H_{F35}
H_{F36}
H_{F37}
H_{F38}

Fig. 4

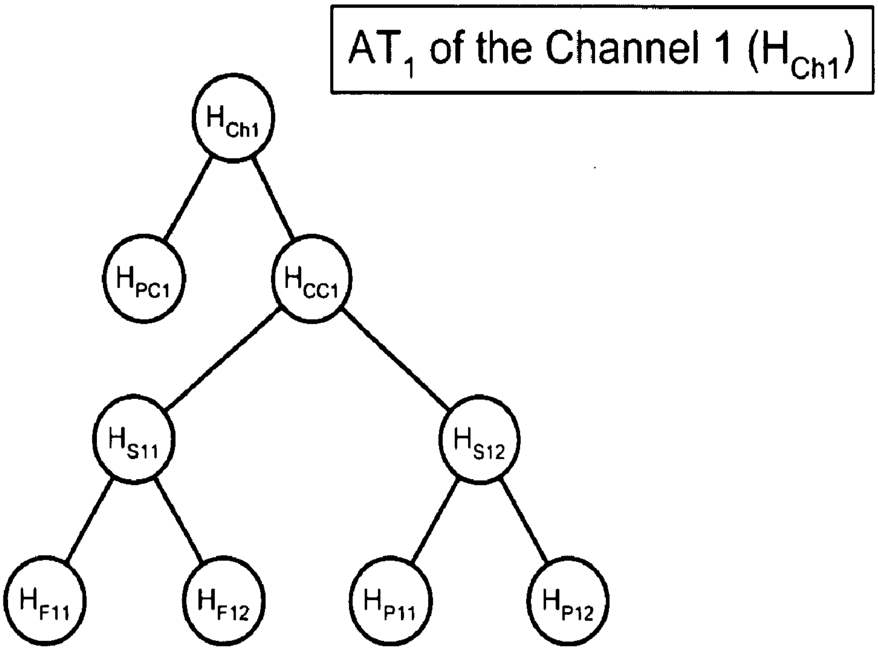

AT_1 of the Channel 1 (H_{Ch1})
H_{Ch1}
H_{PC1}
H_{CC1}
H_{S11}
H_{S12}
H_{F11}
H_{F12}
H_{P11}
H_{P12}

Fig. 5a

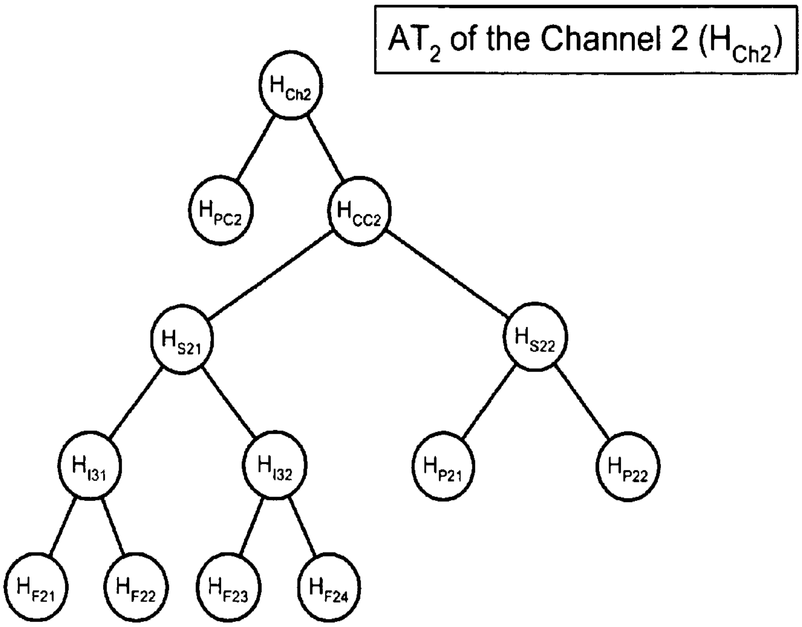

AT_2 of the Channel 2 (H_{Ch2})
H_{Ch2}
H_{PC2}
H_{CC2}
H_{S21}
H_{S22}
H_{I31}
H_{I32}
H_{P21}
H_{P22}
H_{F21}
H_{F22}
H_{F23}
H_{F24}

Fig. 5b

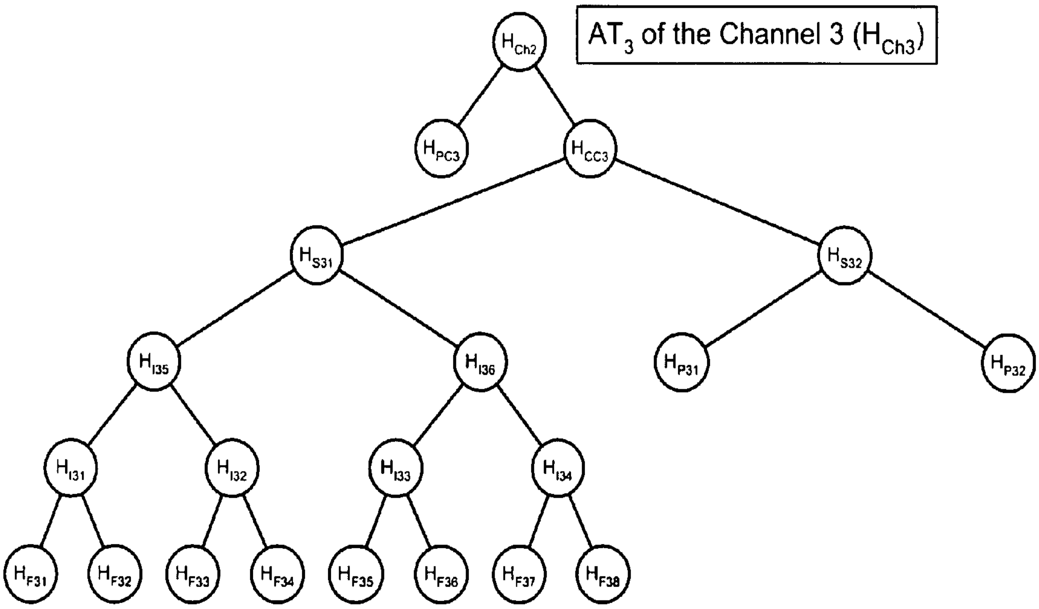
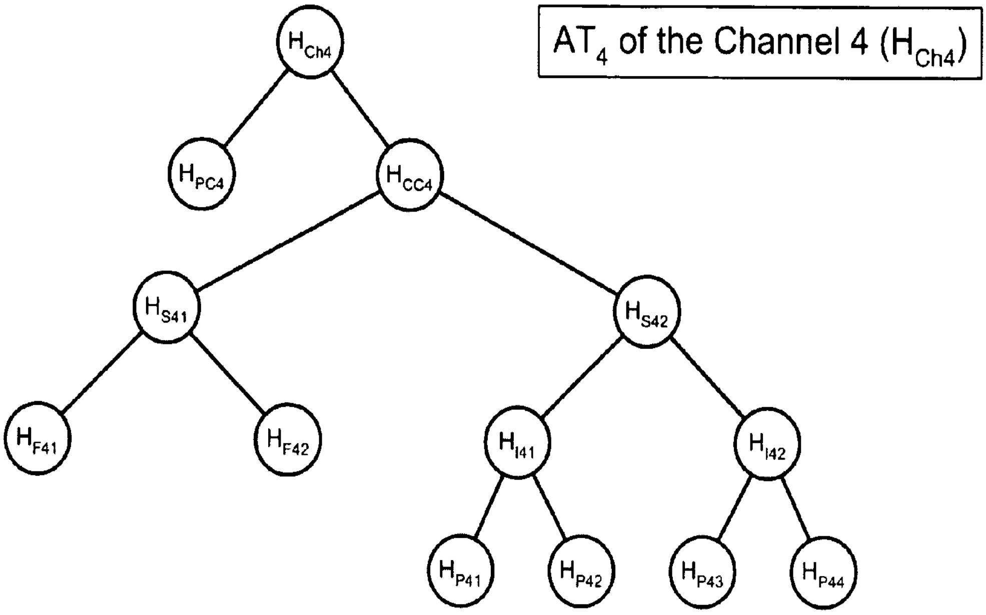
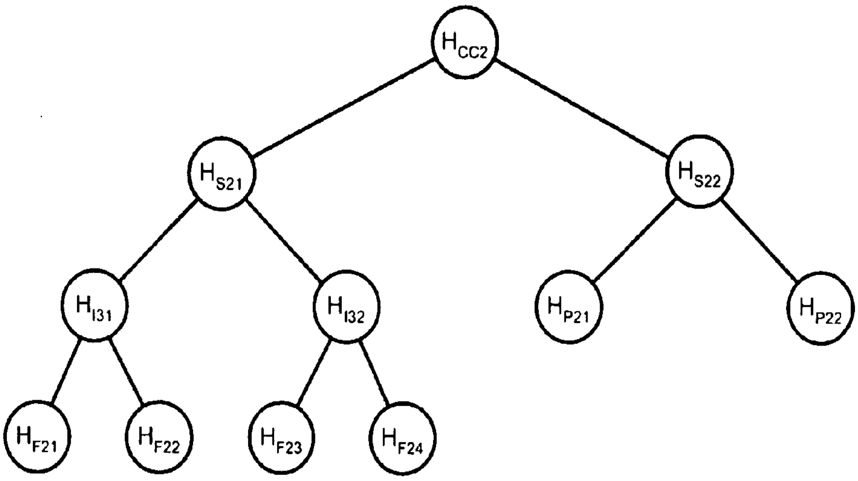

AT_3 of the Channel 3 (H_{Ch3})
H_{Ch2}
H_{PC3}
H_{CC3}
H_{S31}
H_{S32}
H_{I35}
H_{I36}
H_{P31}
H_{P32}
H_{I31}
H_{I32}
H_{I33}
H_{I34}
H_{F31}
H_{F32}
H_{F33}
H_{F34}
H_{F35}
H_{F36}
H_{F37}
H_{F38}

Fig. 5c



AT_4 of the Channel 4 (H_{Ch4})
H_{Ch4}
H_{PC4}
H_{CC4}
H_{S41}
H_{S42}
H_{F41}
H_{F42}
H_{I41}
H_{I42}
H_{P41}
H_{P42}
H_{P43}
H_{P44}

Fig. 5d



H_{CC2}
H_{S21}
H_{S22}
H_{I31}
H_{I32}
H_{P21}
H_{P22}
H_{F21}
H_{F22}
H_{F23}
H_{F24}

Fig. 6a

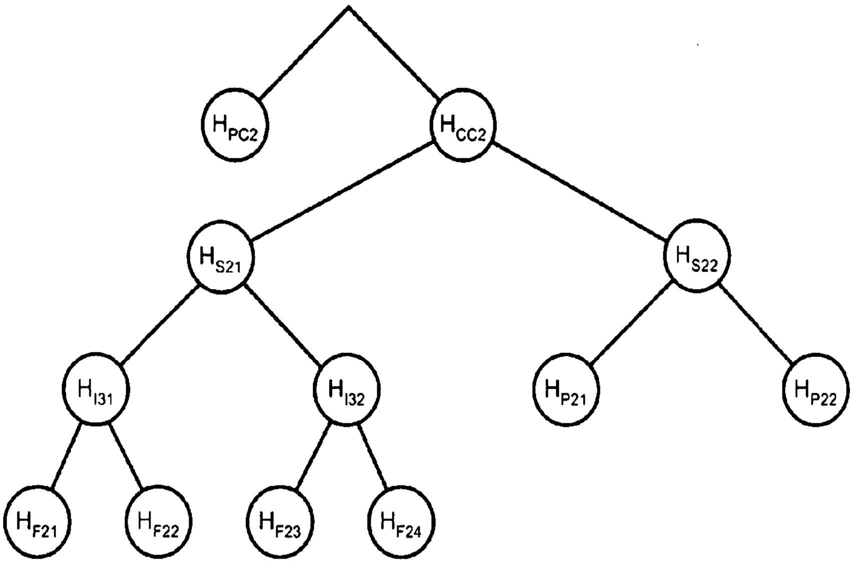

H_{PC2}
H_{CC2}
H_{S21}
H_{S22}
H_{I31}
H_{I32}
H_{P21}
H_{P22}
H_{F21}
H_{F22}
H_{F23}
H_{F24}

Fig. 6b

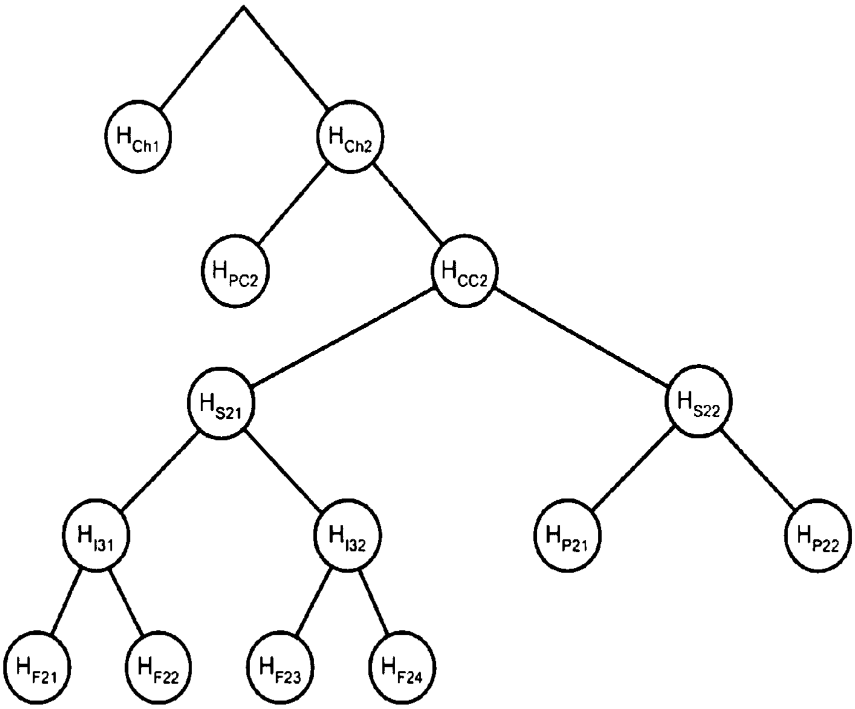

H_{Ch1}
H_{Ch2}
H_{PC2}
H_{CC2}
H_{S21}
H_{S22}
H_{I31}
H_{I32}
H_{P21}
H_{P22}
H_{F21}
H_{F22}
H_{F23}
H_{F24}

Fig. 6c

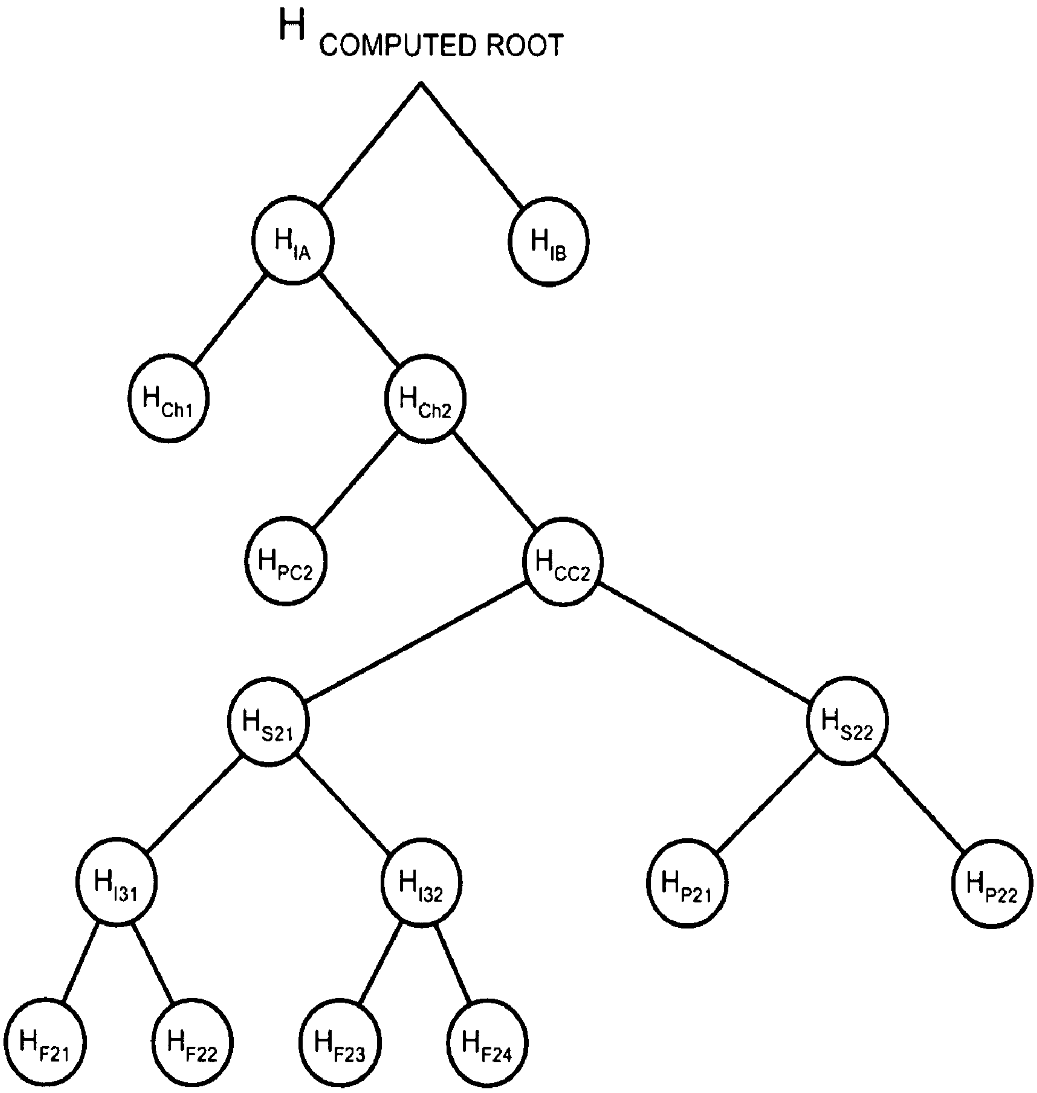

H COMPUTED ROOT
H_IA
H_IB
H_Ch1
H_Ch2
H_PC2
H_CC2
H_S21
H_S22
H_I31
H_I32
H_P21
H_P22
H_F21
H_F22
H_F23
H_F24

Fig. 6d

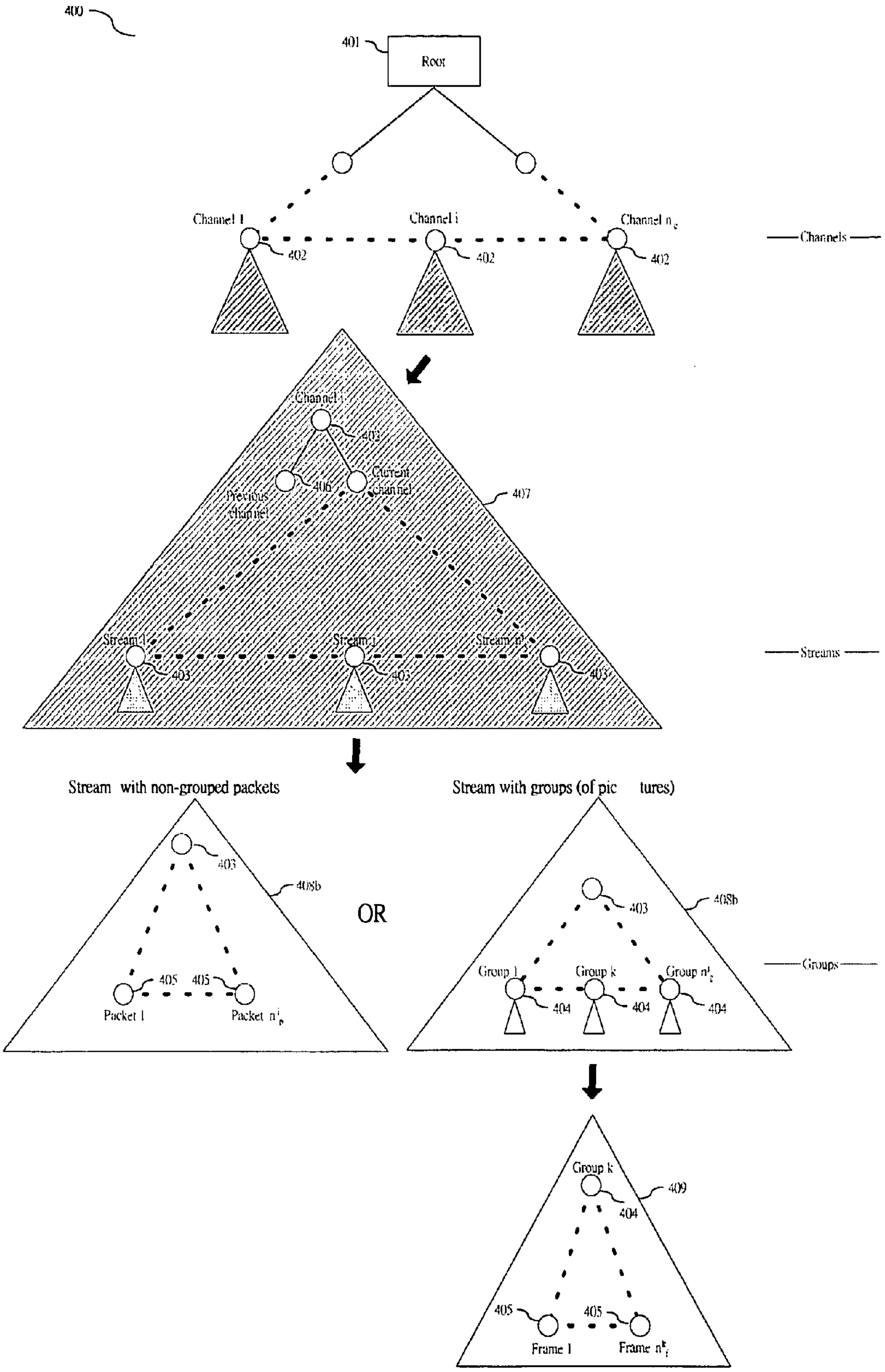

400
401
Root
Channel 1
Channel i
Channel n_c
402
402
402
Channels
Channel i
403
Previous channel
406
Current channel
407
Stream 1
Stream j
Stream n^i_s
403
403
403
Streams
Stream with non-grouped packets
Stream with groups (of pictures)
403
408b
OR
403
408b
405
405
Packet 1
Packet n^j_p
Group 1
Group k
Group n^j_g
404
404
404
Groups
Group k
409
404
405
405
Frame 1
Frame n^k_f

Fig. 7

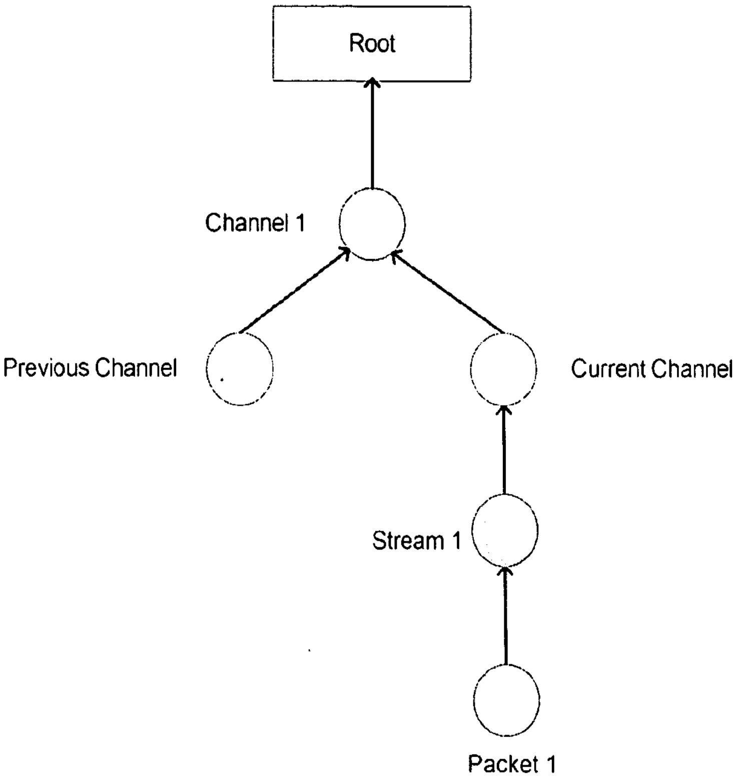

Root
Channel 1
Previous Channel
Current Channel
Stream 1
Packet 1

Fig. 7a

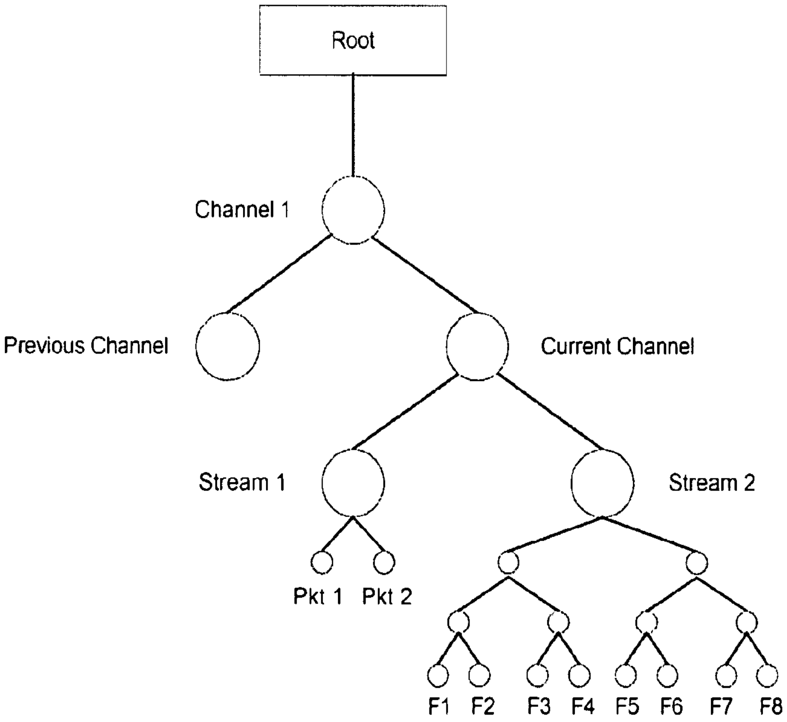

Root
Channel 1
Previous Channel
Current Channel
Stream 1
Stream 2
Pkt 1
Pkt 2
F1
F2
F3
F4
F5
F6
F7
F8

Fig. 7b

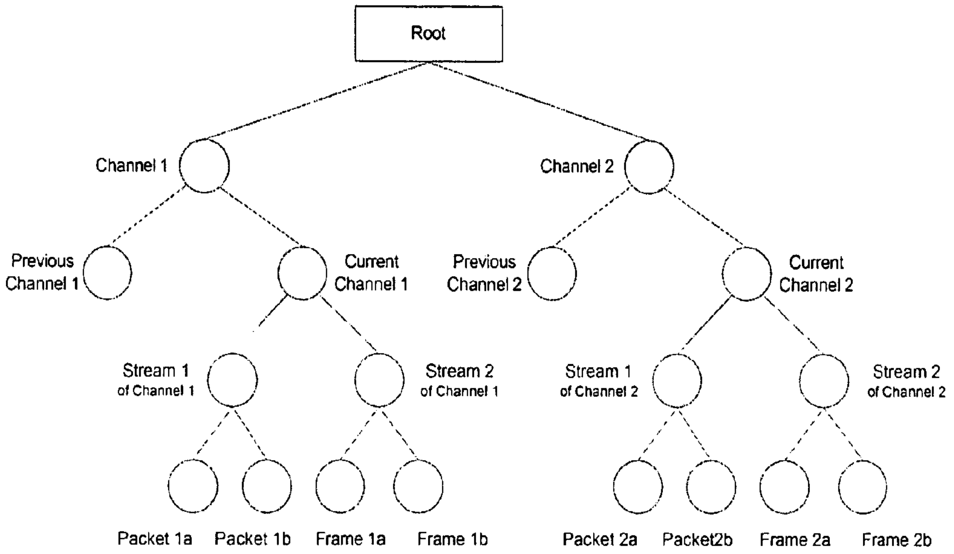


Fig. 7c

VSB* for Time Interval n	VSB for Time Interval n-1	....	VSB for Time Interval 3	VSB for Time Interval 2	VSB for Time Interval 1

* VSB = Video Signature Block

Fig. 8

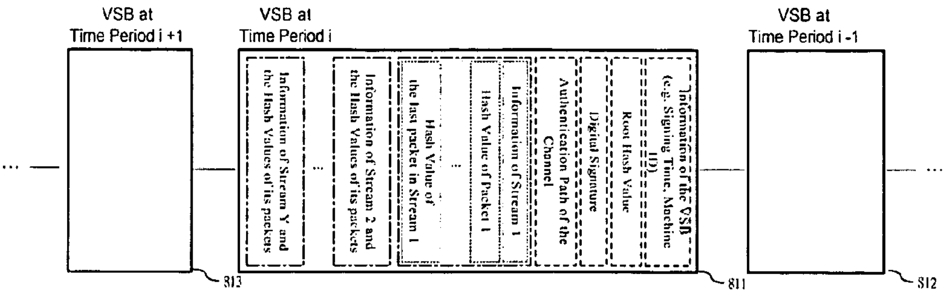

VSB at Time Period i +1
VSB at Time Period i
VSB at Time Period i -1
Information of the VSB (e.g. Signing Time, Machine ID)
Root Hash Value
Digital Signature
Authentication Path of the Channel
Information of Stream 1
Hash Value of Packet 1
Hash Value of the last packet in Stream 1
Information of Stream 2 and the Hash Values of its packets
Information of Stream Y and the Hash Values of its packets
813
811
812

Fig. 8a

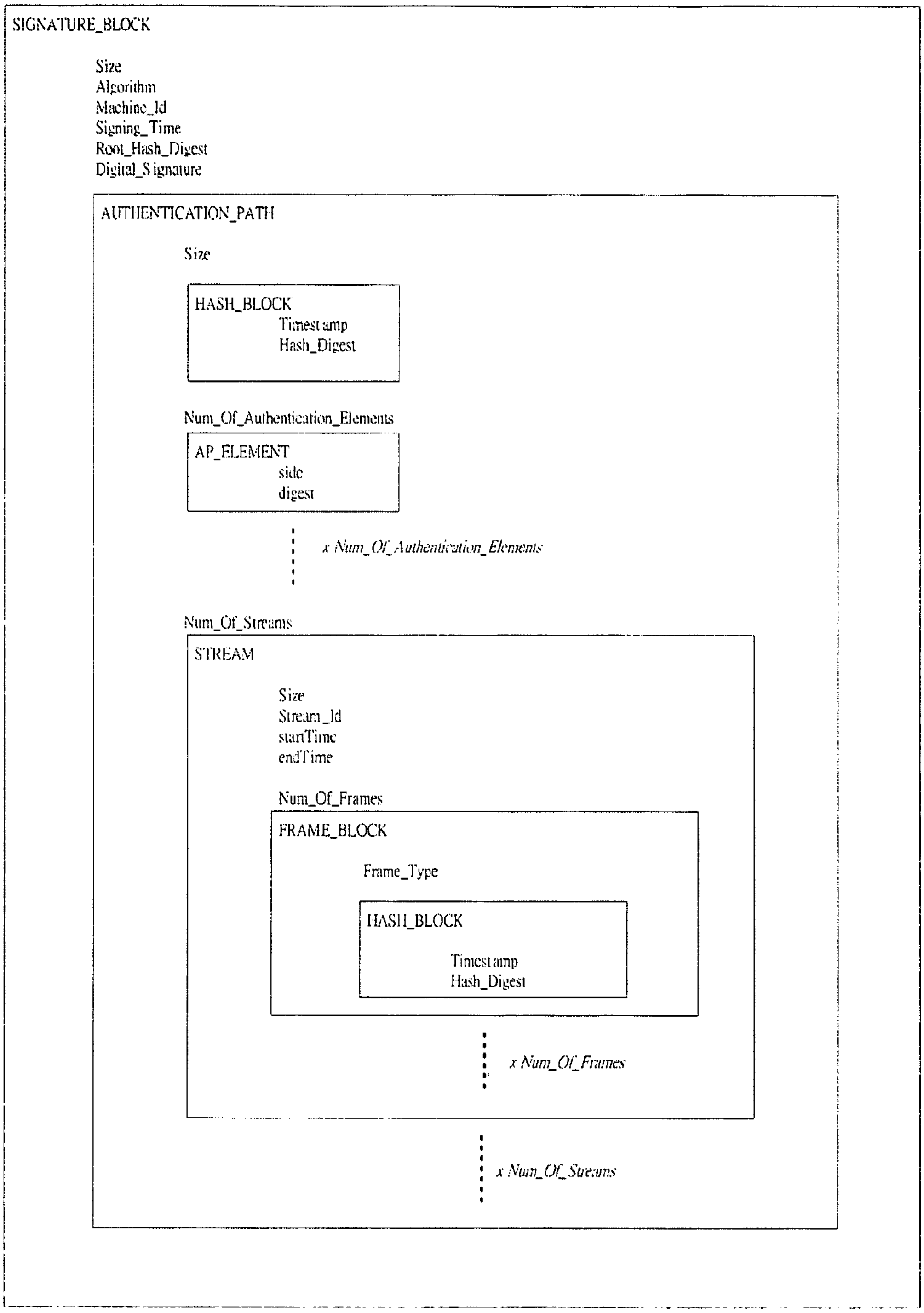

SIGNATURE_BLOCK
Size
Algorithm
Machine_Id
Signing_Time
Root_Hash_Digest
Digital_Signature
AUTHENTICATION_PATH
Size
HASH_BLOCK
Timestamp
Hash_Digest
Num_Of_Authentication_Elements
AP_ELEMENT
side
digest
x Num_Of_Authentication_Elements
Num_Of_Streams
STREAM
Size
Stream_Id
startTime
endTime
Num_Of_Frames
FRAME_BLOCK
Frame_Type
HASH_BLOCK
Timestamp
Hash_Digest
x Num_Of_Frames
x Num_Of_Streams

Fig. 8b

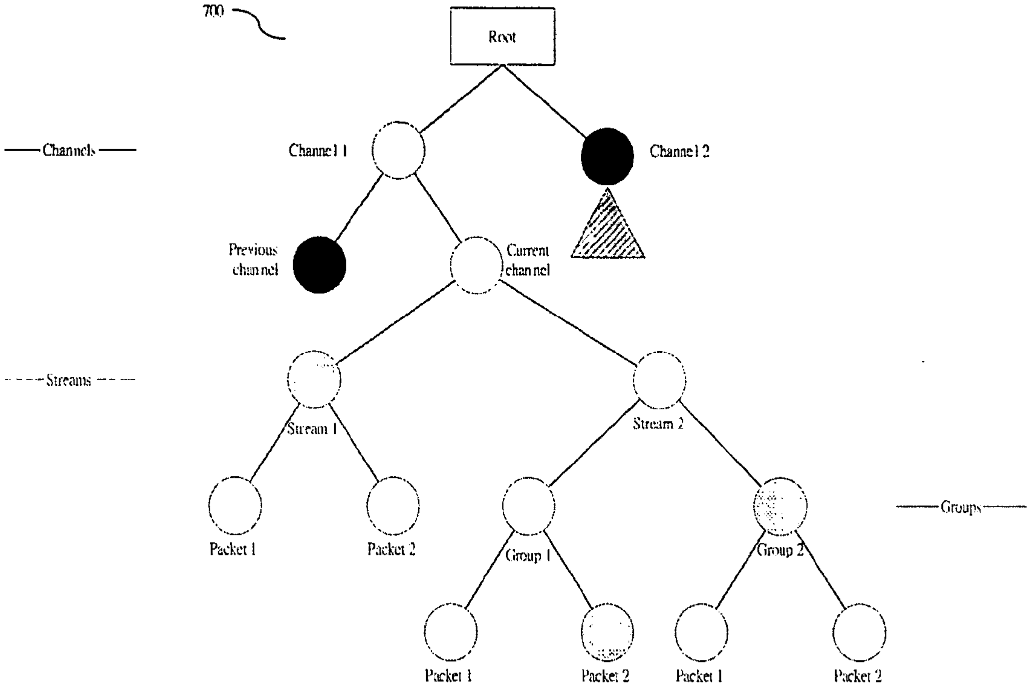
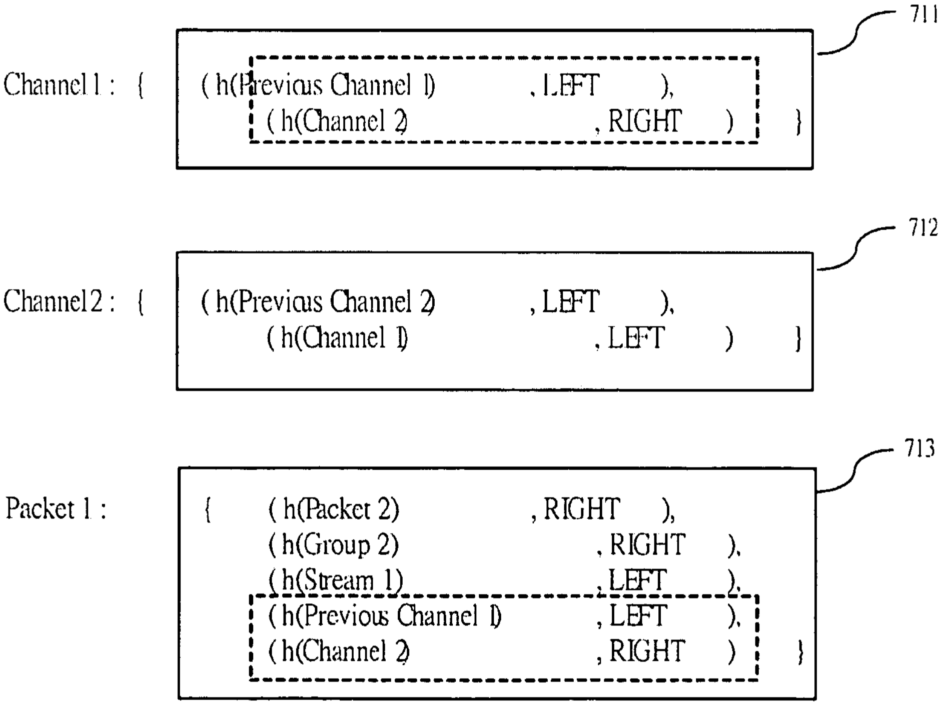


Fig. 9a



```
Channel 1 :  {  ( h(Previous Channel 1)      , LEFT      ),
                  ( h(Channel 2)               , RIGHT     )  }

Channel 2 :  {  ( h(Previous Channel 2)      , LEFT      ),
                  ( h(Channel 1)               , LEFT      )  }

Packet 1 :   {    ( h(Packet 2)              , RIGHT     ),
                  ( h(Group 2)                 , RIGHT     ),
                  ( h(Stream 1)                , LEFT      ),
                  ( h(Previous Channel 1)      , LEFT      ),
                  ( h(Channel 2)               , RIGHT     )  }
```

Fig. 9b

SYSTEM AND METHOD FOR FAST AND SCALABLE MULTIMEDIA AUTHENTICATION IN REAL TIME ENVIRONMENT

FIELD OF THE INVENTION

[0001] This invention relates to authentication of digital medium data. More particularly, the present invention relates to authentication of multi-medium data for secured transportation.

BACKGROUND OF THE INVENTION

[0002] The use of digital data for carrying a medium information, such as pictures, audio and video, has become widespread since the 1990's. With the advent of high performance processors at low costs and more efficient data compression techniques, equipment for converting medium information into digital data files, for example, digital cameras, digital video equipment and MPEG compatible devices, are available to the general public at very affordable costs while offering reasonable or high performance. The proliferation of internet users in recent years plus the ease and convenience associated with the transportation of digital medium files on the internet have rapidly made digital medium as the main stream for use by the general public.

[0003] As medium information is carried by digital data in the digital world and tampering of digital data files is always a concern in the digital information technology world, issues relating to authentication of digitized medium information have become increasingly important. In general, authentication is the process of proving the identity or authenticity of the content, owner and creation date of a document or a piece of information. Data authenticity is of particular importance if a medium information carries certain evidential value. Photographs or moving pictures, for example, those recorded by a surveillance camera, may be used as evidence in support of criminal prosecution or for investigative purposes. In such circumstances, the integrity and authenticity of the data will come under close examination and scrutiny, and the authenticity of the medium information may be pivotal in such cases.

[0004] In the physical world, the question of authenticity can be examined by the more traditional forensic methods which are based on examination of the physical and/or chemical properties of a piece of evidence. In the digital world, however, information is carried in a digital format comprising data of the form "1" or "0". It is well known that digital data is prone to tampering unless security or authentication schemes are applied.

[0005] For authentication of digital medium information, especially digital multimedia authentication, there are two main types of authentication mechanisms, namely, digital watermarking and digital signature. Digital signature is a kind of stenography and is a technology characterized by the injection of hidden information into multimedia data. Although digital watermarking is known to be reasonably robust and tamper resistive, its security relies on a secret key which must be presented for retrieving the watermark. The requirement of a secret key means a digital watermark cannot be publicly verifiable. A disadvantage of digital watermarking is that it can only provide a relatively weak authentication as the exact location at which modification of the medium information has occurred cannot be detected.

[0006] Digital signature is based on cryptographic methods, especially public key cryptography (PKC), is widely used for authentication applications. An authentication scheme utilizing public key cryptography utilizes a private key to send a message and then a public key is used to verify the authenticity of the message. RSA, Diffie-Hellman Elliptic curve and El-Gamal are the better-known algorithms commonly used in public key cryptography. Although digital signature provides for a very useful tool for authentication, an efficient generation of a digital signature for video data application is difficult to achieve using this technique. In particular, the necessary logic calculation cannot be performed efficiently by a video hardware because the calculation usually requires modular exponentiation for a large integer.

[0007] Furthermore, for many real-time applications, the rate of media or multimedia data generation from a source can be prohibitively high so that neither a digital watermarking scheme nor the digital signatures are provide appropriate suitable techniques.

[0008] It is an object of the present invention to provide a method of processing medium data files which overcomes at least some of the disadvantages associated with the techniques of the prior art.

SUMMARY OF THE INVENTION

[0009] Broadly speaking, the present invention has described a method of a method of processing a plurality of digital data files including at least one group of medium data files for constituting a sequence of events or activities of a time interval for secure delivery of the digital data files, the method comprising the steps of:—

[0010] a) processing a plurality of digital data files so as to generate a file identification value for each digital data file, wherein the file identification value of a digital data file is an one-way arithmetic value characteristic of the data content of the digital data file;

[0011] b) processing the file identification values to generate an authentication root value, the authentication root value being an one-way arithmetic value characteristic of the plurality of file identification values;

[0012] c) encrypting the root value; and

[0013] d) grouping the encrypted authentication root value and a selected plurality of digital data files with a set of authentication information for delivery, wherein the set of authentication information is derived from the file identification values and is for deriving a test root value when in combination with said selected plurality of digital data files, and wherein the test root value is for comparison with the authentication root value to detect tampering of said selected plurality of data files.

[0014] This method obviates the need of a digital signature for each individual medium data file so that security transportation can be achieved at a relatively low computational overhead and at the same time facilitating public verification of the data content.

[0015] Preferably, the method comprises construction of an authentication tree from said digital data files, said authentication tree having a root characterized with said root value, a plurality of leave nodes formed from the file identification values of said plurality of digital data files and a plurality of intermediate nodes derived from said leave nodes through one-way arithmetic operations of said file identification values, said intermediate nodes being intermediate the leave nodes and the root, said authentication tree being characterized by a plurality of authentication paths and each intermediate node is associated with an authentication path providing for establishment of the root value of the authentication tree from said intermediate node and the associated authentication paths associated with said intermediate node, the authentication path of an intermediate node is characterized by intermediate nodes which are siblings of said intermediate node, wherein said selected plurality of digital data files which are grouped for delivery comprising a plurality of medium data files for constituting a group of pictures and being under an intermediate node. The employment of a tree structure, especially a binary tree structure, facilitates an efficient authentication scheme particularly suitable for video and/or multi-medium applications.

[0016] Preferably, the root value of the authentication tree is encrypted by a digital signature scheme. This ensures a secured transmission of the root value for reliable authentication at destination.

[0017] Preferably, the file identification value of a digital medium data file is generated by one-way function such as a hash function. The use of one-way functions alleviates the risk of tampering of the individual medium data files.

[0018] Preferably, the medium data files comprise moving picture files or video data files. This method is particularly attractive for video application since a video recording is characterized by a voluminous generation of video data in a short period of time so that generation of individual digital signature for each picture frame or packet would be computationally extensive and impractical.

[0019] Preferably, wherein the video data files is in MPEG-4 or like formats.

[0020] Preferably, a plurality of medium data files and with their corresponding authentication paths are grouped for subsequent transmission, the plurality of medium data files forms moving pictures of a predetermined time period. This method is particularly advantageous for video recording comprising medium data files arranged in groups of pictures so that a single digital signature will be sufficient for a group of pictures.

[0021] According to another aspect of this invention, there is provided a method of verifying integrity of medium data files transmitted according to the aforementioned methods and comprising the steps of:—

[0022] a) decrypting a received root value;

[0023] b) calculating the file identification values from the received medium data files;

[0024] c) calculating a root value from said file identification values and said set of authentication information by one-way arithmetic operations; and

[0025] d) comparing for equality the calculated root value and the received encrypted root value.

[0026] According to yet another aspect of this invention, there is provided an apparatus for processing digital medium data files for transmission, the apparatus comprising:—

[0027] a) a hash value generator for processing a plurality of digital medium data files so as to generate a plurality of file identification values, the file identification value of a digital medium data file is characteristic of its medium data;

[0028] b) an authentication tree generator for processing the plurality of file identification values to form an authentication tree, the authentication tree having a root with a root value and with the plurality of digital medium data files forming leaves of the authentication tree, the authentication tree being characterized by a plurality of authentication paths, each digital medium data file being associated with an authentication path such that the root value of the authentication tree can be established from an digital medium data file and its associated authentication path;

[0029] c) an encryption unit for encrypting the root value of the authentication tree; and

[0030] d) a group unit for grouping the encrypted root value, a plurality of digital medium data files and their respective associated authentication paths for transmission

[0031] According to yet another aspect of this invention, there is provided an apparatus for verifying integrity of medium data files transmitted according to the aforementioned method and comprising:—

[0032] a) a decryption unit for decrypting received root value;

[0033] b) processing unit for calculating the file identification values from the received medium data files;

[0034] c) a processing unit for constructing an authentication tree using the file identification values and the authentication paths received and calculating a root value of the authentication tree; and

[0035] d) a comparison unit for comparing for equality the calculated root value and the received encrypted root value.

BRIEF DESCRIPTION OF THE DRAWINGS

[0036] Preferred embodiments of the present invention will be explained in further detail below by way of example and with reference to the accompanying drawings, in which:—

[0037] FIG. **1** is a schematic diagram showing a multichannel video capturing system with picture processing means for secure transmission in a first preferred embodiment of this invention,

[0038] FIG. **2** is a schematic diagram showing a complete authentication tree for the system of FIG. **1**,

[0039] FIGS. **3***a*, **3***b*, **3***c* and **3***d* respectively show the schematic authentication tree of channels **1**, **2**, **3** and **4** of the video system of FIG. **1**,

[0040] FIG. **4** shows an authentication tree for the video system of FIG. **1** in a second preferred embodiment of this invention,

[0041] FIGS. **5***a*, **5***b*, **5***c* and **5***d* respectively show a schematic authentication tree for channels **1**, **2**, **3** and **4** of the video system of FIG. **1** in a second preferred embodiment of this invention,

[0042] FIG. **6***a* is a schematic diagram showing the reconstruction of a partial authentication path as an intermediate step for verifying the authenticity of a plurality of received medium content data files,

[0043] FIG. **6***b* shows yet a further step in the reconstruction of a partial authentication tree from the partial authentication path of FIG. **6***a,*

[0044] FIG. **6***c* shows a further step of reconstruction of a partial authentication tree from that of FIG. **6***b,*

[0045] FIG. **6***d* shows a final step in the reconstruction of an authentication path up to the computation of the root value for verification of the received medium data file characterized with the hash values of FIG. **6***a,*

[0046] FIG. **7** shows a schematic authentication tree illustrating a third preferred embodiment of this invention,

[0047] FIG. **7***a* shows an exemplary partial authentication tree for packet **1** of stream **1** of FIG. **7**,

[0048] FIG. **7***b* shows an exemplary authentication tree of Channel **1** of FIG. **7**,

[0049] FIG. **7***c* shows another exemplary authentication tree of Channel **1** and Channel **2** of FIG. **7**,

[0050] FIG. **8** is a schematic diagram showing a series of VSBs,

[0051] FIG. **8***a* shows in detail an exemplary VSB,

[0052] FIG. **8***b* shows an exemplary data structure of a VSB,

[0053] FIG. **9***a* illustrates yet another exemplary authentication tree, and

[0054] FIG. **9***b* illustrates the authentication path information for Channel **1**, Channel **2** and Packet **1** of the exemplary authentication tree of FIG. **9***a.*

DETAILED DESCRIPTION OF THE INVENTION

[0055] Referring to the drawings, and more particularly to FIG. **1**, an embodiment of a video capturing system according to the present invention is shown which comprises a plurality of picture capturing devices, an encoder, a controller and an authentication unit. Each picture capturing device is adapted for capturing an optical image and for converting the captured optical image into a stream of digital data, such as a digital video content file. A more sophisticated picture capturing device may comprise a means for outputting a digital multi-medium data file containing additional information such as audio, text, motion vector, timestamp and identity of the picture capturing device in addition to video data. A basic capturing device can be a pin-hole camera while a more sophisticated picture capturing device may comprise a video recorder with an audio input and a data bank for supplying time and identity information.

[0056] The encoder is adapted for converting a digital medium content file into an encoded or compressed data file. The output of the encoder is fed into the controller which is adapted for controlling the picture recording process and the transmission of the encoded digital medium content files.

[0057] The authentication unit comprises a hash generation unit and a signature generation unit. The hash generation unit is adapted to generate a file identification value from a digital medium content file. A file identification value of a digital medium content file is characteristic of its medium content. Typically, a file identification value of a digital medium content file is a hash value generated by a one-way function, such as a hash function, by processing the medium data contained in the file. The timestamp can be used as a unique index of a specific data file in a stream of data file. The output hash value, the timestamp, the channel ID and the stream ID will be sent to the signature generation unit for processing. After the hash values have been calculated, an authentication tree is built.

[0058] The authentication tree is built on the medium data files with the file identification values of the individual medium data files as the leaves. The Merkle Hash Tree, initially described in the article: "A Digital Signature Based On a Conventional Encryption Function", *R. Merkle, Proceedings of Crypto* '87, pp. 369-378, and then described in the article "Fractal Merkle Tree Representation and Traversal" by M. Jakobsson, T Leighton, S. Micali, and M. Szydlo, published on wwwrsasecurity.com, is an example of a suitable authentication tree for this application. The two published articles are incorporated herein by reference.

[0059] More particularly, the authentication tree is built with the hash values of the individual medium data files as the leaves. The leaves are grouped and processed to form intermediate or interior nodes which are in turn grouped and processed until a single root is generated. A plurality layers of intermediate nodes are formed depending on the number of leaves and each node layer is denoted by a layer height. For an authentication tree with a complete binary tree structure, the tree has height H and it has 2H leaves and 2^H-1 interior nodes. The node heights range from "zero" (leaves) to "H" (the root) and the parent's interior node values are one-way functions of the children's interior node values such that:—

$$P(n_{parent})=hash(P(n_{left})\|P(n_{right})),$$

[0060] where the altitude of any node n is the height of the maximum subtree for which it is the root, hash denotes the one-way function and a possible one-way function is SHA-1, MD2, MD5 and other appropriate hash functions. In addition, there is an assignment of a string of a predetermined length to each node in accordance with established hash functions. After the root value has been generated, a video signature will be generated.

[0061] To generate a video signature, the hash values together with the various identification information will be sent to the signature generation unit. The identification information may include, for example, the timestamp, channel identification and stream type identification for a particular data block.

[0062] The signature generation unit will store the hash values and the identification information of a data block in its storage, such as its memory device. When a predetermined number of digital medium content files have been received, for example, a set of digital medium content files retained within a specific time interval of say, 5 seconds, the signature generation unit will construct an authentication tree so that the medium content files can be subsequently authenticated.

[0063] FIG. **2** shows an authentication tree of FIG. **1** in a first preferred embodiment for a specific time interval. In this preferred embodiment, multi-medium data, for example, video data, audio data and text-overlay, are output from the capturing devices. The multi-medium data comprises basic building blocks of "frames" and "packets". Frames are generated sequentially in chronological order and are the building blocks of a video data stream. Other data are typically arranged in packets. The exemplary system of FIG. **1** comprises a plurality of picture capturing devices each of which forms a multi-medium data channel. Such a channel generates a plurality of medium data streams, which can be for example, audio, video or text-overlay.

[0064] For the specific time interval, the video and/or multi-medium data collected by the individual picture capturing devices after encoding and compression are as follows: —

Channel **1**—2 frames, namely, F_{11}, F_{12}

[0065] 2 packets, namely, P_{11}, P_{12}

Channel **2**—4 frames, namely, F_{21}, F_{22}, F_{23}, F_{24}

[0066] 2 packets, namely, P_{21}, P_{22}

Channel **3**—8 frames, namely, F_{31}, F_{32}, F_{33}, F_{34}, F_{35}, F_{36}, F_{37}, F_{38}

[0067] 2 packets, namely, P_{31}, P_{32}

Channel **4**—2 frames, namely, F_{41}, F_{42}

[0068] 4 packets, namely, P_{41}, P_{42}, P_{43}, P_{44}

[0069] In this example, the group of medium files comprising frames F_{11}, F_{12} and packets P_{11}, P_{12} together constitute a sequence of events or activities, such as a video stream or an audio stream. Likewise, the group of medium files comprising frames F_{21}, F_{22}, F_{23}, F_{24} and packets P_{21}, P_{22} together constitute another sequence of events or activities of Channel **2**. When the medium content files arrived at the controller, they are fed into the hash generation unit and the hash values are generated as follows: —

[0070] Channel **1**—H_{F11}, H_{F12}, H_{P11}, H_{P12}

[0071] Channel **2**—H_{F21}, H_{F22}, H_{F23}, H_{F24}, H_{P21}, H_{P22}

[0072] Channel **3**—H_{F31}, H_{F32}, H_{F33}, H_{F34}, H_{F35}, H_{F36}, H_{F37}, H_{F38}, H_{P31}, H_{P32}

[0073] Channel **4**—H_{F41}, H_{F42}, H_{P41}, H_{P42}, H_{P43}, H_{P44}

[0074] Throughout this specification, the capital H is used as a symbol for hash operator. For example, the symbol H_{Fnn} or H_{Pnn} means the hash value of F_{nn} or P_{nn}. The term "medium data file" and "medium data file" is interchangeable used.

[0075] For secure transportation of the medium content files, a plurality of outputs each comprising (1) a leaf pre-image, which is a medium content file giving rise to the leave; and (2) the authentication path of the leaf, i.e., the values of all nodes that are siblings of nodes on the path between that leaf and the root, are generated and delivered. To verify the value of a medium content file, that is, a leaf pre-image, the potential values of the ancestors are calculated by iterated hashing utilizing the authentication path and a leaf pre-image is accepted as authentication if and only if the computed root value is equal to the known root value which is transported. The component authentication trees for the construction of the entire authentication tree are described below. Specifically, the Authentication Tree (AT) of the current Channel **1** is shown in FIG. **3**.

[0076] In FIG. **3***a*, the nodes H_{F11}, H_{F12}, H_{P11}, H_{P12} are leaf nodes and the nodes H_{S11}, and H_{S12} are intermediate nodes each having a characteristic intermediate node value which is derived from a one-way arithmetic operation on the immediately depending leaves. Specifically, H_{S11} is a hash value of H_{F11} & H_{F12} obtained from an appropriate hash function and H_{S12} is a hash value of H_{p11} & H_{p12} obtained from the same hash function. The channel node hash value (H_{Ch1}) is a hash value of the intermediate node hash values H_{S11} and H_{S12}. Similarly, the AT for other channels are shown in FIGS. **3***b*, **3***c* and **3***d*.

[0077] In FIG. **3***b*, the nodes H_{F21}, H_{F22}, H_{F23}, H_{F24}, H_{P21}, H_{P22} are leaf nodes of AT_2, the nodes H_{I21}, H_{I22}, H_{S21} and H_{S22} are intermediate nodes each having a characteristic intermediate node value which is derived from a one-way arithmetic operation on the immediately depending leaves. Specifically, H_{I21} is a hash value of H_{F21} & H_{F22}, H_{I22} is a hash value of H_{F23} & H_{F24}, and H_{S22} is a hash value of H_{P11} & H_{P12}. Also, H_{S21} is a hash value of the intermediate node hash values H_{I21}, H_{I22}. The channel node hash value (H_{Ch2}) is a hash value of the intermediate node hash values H_{S21} and H_{S22}. Similarly, the authentication tree for Channels **3** & **4**, namely, AT_3 & AT_4, are shown respectively in FIGS. **3***c* and **3***d* and the same symbol convention applies as used previously.

[0078] The complete AT of this specific time interval is constructed by the authentication trees of the 4 channels as shown in FIG. **2**.

[0079] Next, the root value of the AT, H_{ROOT}, is digitally signed. The Authentication Paths (AP) for the channels are computed as follows:—

[0080] Channel **1**: {(H_{Ch2}, RIGHT), (H_{IB}, RIGHT)}

[0081] Channel **2**: {(H_{Ch1}, LEFT), (H_{IB}, RIGHT)}

[0082] Channel **3**: {(H_{Ch4}, RIGHT), (H_{IA}, LEFT)}

[0083] Channel **4**: {(H_{Ch3}, LEFT), (H_{IA}, LEFT)}

[0084] When the digital medium content files, for example, F_{11}, F_{12}, P_{11}, and P_{12} in case of Channel **1**, are sent with the relevant AP, that is, the AP for Channel **1**, a root value can be computed for verification with the publicly received and signed root value.

[0085] In a second preferred embodiment of the multi-medium system of FIG. **1**, the contents of the immediately preceding interval of each of the channels are used to build the authentication tree. Specifically, the hash values of each of the channels of the immediately preceding time interval are used. In the following H_{PCn} means the hash value of the immediately preceding hash value of channel n and the authentication trees are as follows:—

[0086] For Channel **1**, AT_1 is as shown in FIG. **5***a*.

[0087] For Channel **2**, AT_2 is as shown in FIG. **5***b*.

[0088] For Channel **3**, AT_3 is shown in FIG. **5***c*.

[0089] For Channel **4**, AT_4 is as shown in FIG. **5***d*.

[0090] The complete authentication tree of this second preferred embodiment is shown in FIG. **4**.

The root value of the AT, H_{ROOT}, is signed digitally and the Authentication Paths (AP) for the channels are computed:—

[0091] Channel **1**: {(H_{PC1}, LEFT), (H_{Ch2}, RIGHT), (H_{IB}, RIGHT)}

[0092] Channel **2**: {(H_{PC2}, LEFT), (H_{Ch1}, LEFT), (H_{IB}, RIGHT)}

[0093] Channel **3**: {(H_{PC3}, LEFT), (H_{Ch4}, RIGHT), (H_{IA}, LEFT)}

[0094] Channel **4**: {(H_{PC4}, LEFT), (H_{Ch3}, LEFT), (H_{IA}, LEFT)}

[0095] In the various partial authentication trees, the following keys apply:—

Keys	

H_{Fii} / H_{Pii}	Leave nodes;
	Frames/packets;

H_{Iii}	Intermediate nodes; (For building up the binary tree, not representing and components;)

H_{Sii}	Intermediate nodes;
	Streams;

H_{CCi}	Intermediate nodes;
	Current channel;

H_{PCi}	Intermediate nodes; Previous channel (channel node on the previous AT of the same channel);
H_{Chi}	Root node of the channel;

[0096] The medium content files are delivered together with a video signature block (VSB) which contains the necessary authentication information. In particular, there is one VSB for one channel in every time interval. Specifically, the Video Signature Blocks for the channels at a specific time interval contain the following:—

[0097] VSB of Channel **1**

[0098] Digital Signature:Signed H_{ROOT}

[0099] Authentication Path:{(H_{PC1}, LEFT), (H_{Ch2}, RIGHT), (H_{1B}, RIGHT)}

[0100] Hash values:H_{F11}, H_{F12}, H_{P11}, H_{P12}

[0101] VSB of Channel **2**

[0102] Digital Signature:Signed H_{ROOT}

[0103] Authentication Path:{(H_{PC2}, LEFT), (H_{Ch1}, LEFT), (H_{1B}, RIGHT)}

[0104] Hash values:H_{F21}, H_{F22}, H_{F23}, H_{F24}, H_{P21}, H_{P22}

[0105] VSB of Channel **3**

[0106] Digital Signature:Signed H_{ROOT}

[0107] Authentication Path:{(H_{PC3}, LEFT), (H_{Ch4}, RIGHT), (H_{IA}, LEFT)}

[0108] Hash values:H_{F31}, H_{F32}, H_{F33}, H_{F34}, H_{F35}, H_{F36}, H_{F37}, H_{F38}, H_{P31}, H_{P32}

[0109] VSB of Channel **4**

[0110] Digital Signature:Signed H_{ROOT}

[0111] Authentication Path:{(H_{PC4}, LEFT), (H_{Ch3}, LEFT), (H_{IA}, LEFT)}

[0112] Hash values:H_{F41}, H_{F42}, H_{P41}, H_{P42}, H_{P43}, H_{P44}

[0113] Upon receipt of the medium content files and the VSB, which contains the authentication information, a recipient of the medium content files can verify the integrity of the received data by reconstruction of the authentication trees based on the received medium content file(s) and the authentication information. For example, assuming the medium files to be verified are from Channel **2**, the frames/packets belonging to a time interval will be verified in a single verification. The data blocks are verified against the VSB generated for that specific time interval) in the following exemplary manner.

Data to be Verified

4 Frames: F_{21}, F_{22}, F_{23}, F_{24}

2 packets: P_{21}, P_{22}

Content of the VSB at Hand

[0114] Digital Signature:Signed H_{ROOT}

[0115] Authentication Path:{(H_{PC2}, LEFT), (H_{Ch1}, LEFT), (H_{IB}, RIGHT)}

[0116] Hash values:H_{F21}, H_{F22}, H_{F23}, H_{F24}, H_{P21}, H_{P22}

Step 1

Calculate the hash values of each element (i.e. F_{21}, F_{22}, F_{23}, F_{24}, P_{21}, P_{22})

Obtained H_{F21}, H_{F22}, H_{F23}, H_{F24}, H_{P21}, H_{P22}

Step 2

Reconstruct the partial Authentication Path with the calculated hash values, as shown in FIG. **6***a*.

Step 3

[0117] Rebuild the root value of Channel **2**, i.e., H_{Ch2}, from the information contained in the Authentication Path of the VSB and using {(H_{PC2}, LEFT), (H_{Ch1}, LEFT), (H_{IB}, RIGHT)}, as shown in FIG. **6***b*.

Next, H_{IA} is derived from {(H_{PC2}, LEFT), (H_{Ch1}, LEFT), (H_{IB}, RIGHT)}, as shown in FIG. **6***c*.

Finally, the root value is computed from {(H_{PC2}, LEFT), (H_{Ch1}, LEFT), (H_{IB}, RIGHT)}, as shown in FIG. **6***d*.

Step 4

Next, the computed root value, $H_{COMPUTED\ ROOT}$ is checked against the Signed H_{ROOT} contained in the received VSB.

The data are considered valid if $H_{COMPUTED\ ROOT}$ is equal to the Signed H_{ROOT}.

[0118] In a third preferred embodiment of this invention, the system is adapted for transmission of multi-medium data comprising video encoded in the MPEG-4 format. The MPEG-4 standard is becoming a popular format for streaming multi-media on the Internet. MPEG-4 encodes a bitstream in groups of different frame types (I, P and B frames), where the I-frame is independent, while the P- and B-frames depend on the I-frame in the group. Specifically, the I-frame is an entire picture frame of video encoded in JPEG and the P-frame contains the "difference" between a subsequent video frame and the previous video frame. Thus, losing an I-frame will cause a noticeable worsening of the video quality of all the frames in the group.

[0119] The MPEG-4 standard arranges video data in groups of pictures (GOP) comprising a single I-frame and a plurality of P-frames. Groups of pictures are demarcated by I-frame intervals, that is, two consecutive I-frames are the bounding frames of a group of pictures and the P-frames in between a pair of consecutive I-frames belong to the same GOP. The use of group of pictures facilitates more efficient video extraction because frames within an I-frame interval (which is generally regarded as the minimum unit for video extraction) are arranged together and can be extracted separately. A schematic authentication tree of this embodiment is shown in FIG. **7** in which the system has been generalized to contain n channels, namely, Channel **1** to Channel n. The authentication tree of each channel (channel i is shown as an example) is built from the hash values of the previous channel and the current channel. The current channel comprises a plurality of data streams, namely, streams **1**, . . . stream j, . . . steam n.

[0120] Each of the streams may be a stream of non-grouped packets or a stream of groups of pictures (GOP). Each grouped stream may comprise a plurality of groups in which each group may in turn comprise a plurality of frames, namely, frames **1**-*n*.

[0121] An exemplary authentication tree of the current channel of Channel **1** comprising stream **1** with packet **1** under stream **1** is shown in FIG. **7***a*. Another exemplary authentication tree of the current channel of Channel **1** comprising streams **1** and **2** with packets **1** and **2** under stream **1** and frames F**1**-F**8** under stream **2** is illustrated in FIG. **7***b*. Alternatively, each of the F**1** to F**8** can comprise a group or groups of pictures of a predetermined time interval. Yet another exemplary authentication tree for Channel **1** and Channel **2** with packet **1***a*, packet **1***b*, frame **1***a* and frame **1***b* under current Channel **1** and packet **2***a*, packet **2***b*, frame **2***a*, frame **2***b* under current Channel **2** is illustrated in FIG. **7***c*.

[0122] The video signature blocks (VSB) for various consequential time intervals are schematically shown in FIG. **8**. A more detailed block diagram of a VSB for a time period I is shown in FIG. **8***a*. The VSB of FIG. **8***a* comprises information of the VSB, such as, for example, the signing time and the machine ID, the root hash value, the digital signature, the authentication path of the channel, information of the streams, information of packets, hash values of the last (previous) packet in stream **1**, information of stream **2** and the hash values of its packets and information of other streams and the hash values of the other streams.

[0123] The data structure of the VSB of FIG. **8***a* in a programming perspective is shown in FIG. **8***b*. In this preferred embodiment, the number of video signatures generated is equal to the number of authentication tree formed, since there is a signature for each authentication tree. In other words, the number of signatures generated does not depend on the amount of data. Instead, the frequency of video signature generation is determined by the system design and is generated at predetermined time intervals. For example, the predetermined time interval may be set at 1 second in which case an authentication tree will be formed per second. In that particular time interval, a number of packets and frames will arrive at different channels. The hash generation unit will calculate the hash values according to the contents of the packets and frames and the hash values are fed to the signature generation unit which in turn forms the basis of a corresponding authentication tree. The root value of the authentication tree will be digitally signed for transmission when the authentication tree is built. The authentication method is particularly efficient for video transmission since a digital signature can be applied for a group of pictures without the need of individual digital signature for each of the I- or P-frames.

[0124] Another important feature of this authentication method is the time-based signature generation. More particularly, to reduce computational overheads, the time intervals between consecutive signature generations can be adjusted in accordance with system requirements. This flexibility enables the method to be applicable to system of different computational power. For example, digital signatures may be generated at the rate of one signature per 10 seconds for a low-end system while the digital signatures may be generated at a higher rate for a higher-end system.

[0125] Furthermore, if a medium content file, for example, packet **1** is tampered, the error in the computed hash values will be propagated upwards to the root. The erroneous hash value when compared with the hash values of the intermediate nodes of the authentication tree can be utilized to facilitate identification of the particular medium content files which has been tampered. This will enable a quick and efficient identification of a particular content file which has been tampered. For example, if the tampered file is a P-frame in the MPEG-4 system, the file may be discarded without seriously affecting the quality of the video whilst maintaining the authenticity of the video compared to traditional schemes in which the digital signature generation rate is dependent on the number of data blocks or the number of multi-media channels, the authentication method of this invention represents a substantial improvement.

[0126] Another exemplary partial authentication tree is shown in FIG. **9***a* in which a complete authentication tree of the current channel of Channel **1** is shown. Specifically, the current channel of Channel **1** comprises stream **1** and stream **2** with packets **1** and **2** arranged under stream **1** and groups of pictures **1** and **2** arranged under stream **2**. The authentication paths for Channel **1**, Channel **2** and packet **1** are shown in FIG. **9***b*. More particularly, it will be noted from FIG. **9***b* that the authentication path information of Channel **1** is also contained in that of packet **1**, as more particularly shown in the dotted boxes in the blocks **711** and **713** of FIG. **9***b*.

[0127] From the above examples, it will be appreciated that although an authentication tree is constructed from multi-medium data streams of the various channels, only the authentication tree root signature, the authentication path information and the medium content data to be authenticated are required to be available during the verification process.

[0128] While the present invention has been explained by reference to the examples or preferred embodiments described above, it will be appreciated that those are examples to assist understanding of the present invention and are not meant to be restrictive. Variations or modifications which are obvious or trivial to persons skilled in the art, as well as improvements made thereon, should be considered as equivalents of this invention.

[0129] Furthermore, while the present invention has been explained by reference to video data or multi-medium data files, it should be appreciated that the invention can apply, whether with or without modification, to other multi-medium data or video only data without loss of generality.

1. A method of processing a plurality of digital data files including at least one group of medium data files for constituting a sequence of events or activities of a time interval for secure delivery of the digital data files, the method comprising the steps of:—

(a) processing a plurality of digital data files so as to generate a file identification value for each digital data file, wherein the file identification value of a digital data file is an one-way arithmetic value characteristic of the data content of the digital data file;

(b) processing the file identification values to generate an authentication root value, the authentication root value being an one-way arithmetic value characteristic of the plurality of file identification values;

(c) encrypting the root value; and

(d) grouping the encrypted authentication root value and a selected plurality of digital data files with a set of authentication information for delivery, wherein the set of authentication information is derived from the file identification values and is for deriving a test root value when in combination with said selected plurality of digital data files, and wherein the test root value is for comparison with the authentication root value to detect tampering of said selected plurality of data files.

2. A method according to claim 1, wherein said set of authentication information for deriving a test root value contains authentication data obtained from one-way arithmetic operation of digital data files not selected for grouping.

3. A method according to claim 1, wherein the selected plurality of digital data files comprising at least a group of medium data files, said group of medium data files comprising a stream of video or moving pictures and/or an audio stream of a time interval.

4. A method according to claim 1, wherein the plurality of digital data files is from a plurality of physical channels and said selected plurality of digital data files selected for delivery comprises a selected group of medium data files from one of said plurality of physical channels, said selected group of medium data files comprising a stream of video or moving pictures and/or an audio stream of a time interval.

5. A method according to claim 4, wherein said set of authentication information for deriving a test root value from said selected plurality of digital data files comprises an intermediate file identification value, said intermediate file identification value being a characteristic value derived from digital data files of another physical channel through one-way arithmetic operations and being characteristic of said digital data files of said another physical channel.

6. A method according to claim 5, wherein said set of authentication information for deriving a test root value comprises an additional intermediate file identification value, said additional intermediate file identification value being a characteristic value derived from digital data files of all remaining physical channel through one-way arithmetic operations and being characteristic of said digital data files of said remaining physical channels.

7. A method according to claim 4, wherein said group of medium data files comprises a picture data file and a plurality of variation data files, each said variation data file containing information of changes with respect to said picture data file, said picture data file and said plurality of variation data files together forming a group of moving picture data files.

8. A method according to claim 7, wherein said group of moving picture data files comprises data files in MPEG-4 or like formats.

9. A method according to claim 1, wherein said group of medium data files constituting a stream of video or moving pictures data files of a current time interval is selected for delivery with said encrypted root value, said group of medium data files being processed by one-way arithmetic operations to generate an intermediate file identification value which is characteristic of said group of medium data files, the intermediate file identification value of said group of medium data files of said current time interval being processed with the intermediate file identification value of the same group of medium data files of a previous time interval for generation of said root value, the intermediate file identification value of said previous time interval being also transmitted as part of said set of authentication information.

10. A method according to claim 1, wherein the plurality of digital data files from a plurality of physical channels, at least some of the physical channels being for sending moving picture data files at various time intervals, the file identification value of a group of medium data files delivered in a previous time interval being processed with that of a current group of medium data files to obtain the root value.

11. A method according to claim 10, wherein the file identification values of the plurality of digital data files from a physical channel being processed to form an intermediate node identification value, the intermediate node identification values of the plurality of physical channels being processed together to form the root value.

12. A method according to claim 1, wherein the file identification value of a digital data file is generated by a one-way function, wherein said one-way function is selected from a group including a hash function.

13. A method according to claim 12, wherein said one-way function is characterized by the return of a hash value of a pre-determined data length irrespective of the content of said digital data file, said hash value being specific to the content of said digital data file.

14. A method according to claim 1, wherein information relating to the time of generation of the medium content files is also grouped and encrypted for delivery of the selected plurality of digital data files, wherein said selected selection plurality of digital files comprises at least one group of said medium data files.

15. A method according to claim 1, wherein the plurality of digital data files being is from a plurality of physical channels and the selected plurality of digital data files is selected for transmission comprising a group of moving picture data files from a physical channel, information relating to identity of said physical channel is also grouped and encrypted for transmission.

16. A method according to claim 15, wherein the medium data file includes multi-media data such as video, audio, text overlay, motion vector and like data.

17. A method according to claim 15, wherein the authentication root value is encrypted by a digital signature scheme before delivery.

18. A method according to claim 15, wherein the digital signature generation is by a publicly verifiable cryptographic key infrastructure.

19. A method according to claim 1, wherein the method comprises construction of an authentication tree from said digital data files, said authentication tree having a root characterized with said root value, a plurality of leave nodes formed from the file identification values of said plurality of digital data files and a plurality of intermediate nodes derived from said leave nodes through one-way arithmetic operations of said file identification values, said intermediate nodes being intermediate the leave nodes and the root, said authentication tree being characterized by a plurality of authentication paths and each intermediate node is associated with an authentication path providing for establishment of the root value of the authentication tree from said intermediate node and the associated authentication paths associated with said intermediate node, the authentication path of an intermediate node is characterized by intermediate nodes which are siblings of said intermediate node, wherein said selected plurality of digital data files which are grouped for delivery comprising a plurality of medium data files for constituting a group of pictures and being under an intermediate node.

20. A method according to claim 19, wherein said group of digital medium data files comprises video data files generated and is transmitted at different time intervals, the authentication path of a later transmitted group of pictures comprising the intermediate node of an earlier transmitted group of digital medium data files.

21. A method according to claim 1, wherein the group of medium data files is provided in AVI format and contains a video signature block, the video signature block comprising file identification values of the medium data files and authentication paths.

22. A method according to claim 21, wherein the medium data files comprises a video signature stream, a video stream, an audio stream, a text overlay stream and a motion vector stream which are multiplexed to form an AVI stream.

23. A method according to claim 21, wherein the video signature block further comprises time information relating to the medium data files.

24. A method of verifying integrity of delivered medium data files processed according to the method of claim 1 and further comprising the steps of:—

e) decrypting a received root value;

f calculating the file identification values from the received medium data files;

g) calculating a root value from said file identification values and said set of authentication information by one-way arithmetic operations; and

h) comparing for equality the calculated root value and the received encrypted root value.

25. An apparatus for processing digital medium data files for transmission, the apparatus comprising:

a) a hash value generator for processing a plurality of digital medium data files so as to generate a plurality of file identification values, the file identification value of a digital medium data file is characteristic of its medium data;

b) an authentication tree generator for processing the plurality of file identification values to form an authentication tree, the authentication tree having a root with a root value and with the plurality of digital medium data files forming leaves of the authentication tree, the authentication tree being characterized by a plurality of authentication paths, each digital medium data file being associated with an authentication path such that the root value of the authentication tree can be established from an digital medium data file and its associated authentication path;

c) an encryption unit for encrypting the root value of the authentication tree; and

d) a group unit for grouping the encrypted root value, a plurality of digital medium data files and their respective associated authentication paths for transmission.

26. An apparatus for verifying integrity of medium data files transmitted according to the method of claim 25 and comprising:—

e) a decryption unit for decrypting received root value;

f) processing unit for calculating the file identification values from the received medium data files;

g) a processing unit for constructing an authentication tree using the file identification values and the authentication paths received and calculating a root value of the authentication tree; and

h) a comparison unit for comparing for equality the calculated root value and the received encrypted root value.

* * * * *