Claims

1. Method to watermark a compressed content received by a client device, said client device receiving an encrypted compressed content, encrypted by at least one content key (CA key), encrypted CAS Data comprising the at least one content key (CA key) and pre-marking data (WMD) ~~which is part of an Entitlement Control Message (ECM)~~ encrypted by a first transmission key, ~~and receiving pre-marking data,~~ said client device comprising:

- a Descrambler (103) having an input to receive the encrypted compressed content and an output to produce a decrypted compressed content,
- a WM inserter (104) directly connected to the output of the Descrambler,

said Descrambler and said WM inserter being connected with ~~the~~ a Conditioner (200), said Conditioner comprising an identifier, said method comprising the following steps :

- receiving the CAS Data~~Entitlement Control Message and the pre-marking data~~,
- decrypting the CAS Data ~~Entitlement Control Message~~ with the first transmission key and extracting the content key (CA key),
- decrypting the pre-marking data,
- verifying the signature of the pre-marking data, and if the signature is valid,
- transferring the pre-marking data and the identifier to the WM inserter,
- validating the content key (CA key) for the descrambler (103),
- watermarking by the WM inserter, the decrypted content received by the descrambler using the pre-marking data and the identifier, said pre-marking data comprising at least one content index, defining the location in which a modification can be made, and at least an alternate value to insert at said location.

2. Method of claim 1, wherein the pre-marking data are organized in packets, each packet comprising a signature and a set or records, each record comprising a content index and an alternate value, for a given content index, the WM inserter deciding to change or to keep the original value of the content at the content index based on a bit of the identifier.

3. Method of any of the claims 1 to 2, wherein the client device comprises a Host CPU in charge of running an operating system, and wherein the Conditioner, the Descrambler and the WM inserter are located in a secure environment and the connections between these elements are not accessible by the Host CPU.

4. Method of claim 1 wherein the pre-marking data are embedded into the encrypted content and decrypted by the ~~CA~~-Descrambler, ~~sais~~ said method comprising the steps of :

- extracting at the output of the ~~CA~~ Descrambler the pre-marking data and transferring them to the Conditioner,

- extracting a signature from the pre-marking data and verifying the signature by the Conditioner.

5. Method of any of the claims 1 to 3, wherein the content key and the pre-marking data are included in ~~the~~ an Entitlement Control Message.

6. Method of any of the claims 2 to 5, wherein the pre-marking record further comprise the original value at the content index, said WM Inserter (104) verifying that the value in the content is the same as the original value of the pre-marking record, and further informing the Conditioner (200) of the result of the verification.

7. Method of any of the claims 1 to 7, wherein the Entitlement Control Message (ECM) comprises access conditions, these access conditions being checked by the Conditioner (200) before the content key is transferred to the ~~CA~~ Descrambler (103).

8. Client device for decrypting and watermarking an encrypted compressed content, said compressed content comprising pre-marking data and being encrypted by at least one content key (CA key), said content key being received by the client device in ~~an Entitlement Control Message (ECM)~~ encrypted CAS Data encrypted by a first transmission key, said client device comprising:

- a Descrambler (103) having an input to receive the encrypted compressed content and an output to produce a decrypted compressed content,

- a Conditioner (200) in charge of receiving the ~~Entitlement Control Message~~ encrypted CAS Data and the decrypted pre-marking data, and decrypting the ~~Entitlement Control Message~~encrypted CAS Data with the first transmission key and extracting the content key (CA key), said Conditioner comprising an identifier,

- a WM inserter (104) directly connected to the output of the Descrambler, in charge of watermarking the decrypted content with the pre-marking data and the identifier, said pre-marking data comprising at least one content index, defining the location in which a modification can be made, and at least an alternate value to insert at said location,

said Descrambler and said WM inserter being connected with the Conditioner (200),

- said Conditioner (200) comprising means to verify a signature of the pre-marking data, and if the signature is valid, means to transfer the pre-marking data and the identifier to the WM inserter, characterized in that, the Descrambler is in charge of decrypting the pre-marking data together with the encrypted content and has means to filter and to direct to the Conditioner the decrypted pre-marking data.