(12) UK Patent (19) GB (11) 2533279 (13) B

(45) Date of B Publication 14.08.2019

(54) Title of the Invention: Secure media player

(51) INT CL: ***H04N 21/2347*** (2011.01) ***G06F 21/10*** (2013.01) ***H04N 21/4405*** (2011.01) *H04N 21/266* (2011.01)

(21) Application No: **1421817.6**

(22) Date of Filing: **08.12.2014**

(43) Date of A Publication **22.06.2016**

(56) Documents Cited:

EP 2346246 A1
EP 2073545 A2
WO 2014/175910 A1
WO 2010/042318 A1
US 20040236940 A1
US 20030152226 A1

(58) Field of Search:

As for published application 2533279 A viz:
INT CL **H04N**
Other: **EPODOC, WPI**
updated as appropriate

Additional Fields
INT CL **G06F**
Other: **None**

(72) Inventor(s):

Tuomas Kärkkäinen
Ossi Mikael Kalevo

(73) Proprietor(s):

Gurulogic Microsystems Oy
Linnankatu 34, Turku FI-20100, Finland

(74) Agent and/or Address for Service:

Basck Ltd
16 Saxon Road, CAMBRIDGE, Cambridgeshire, CB5 8HS, United Kingdom

GB 2533279 B

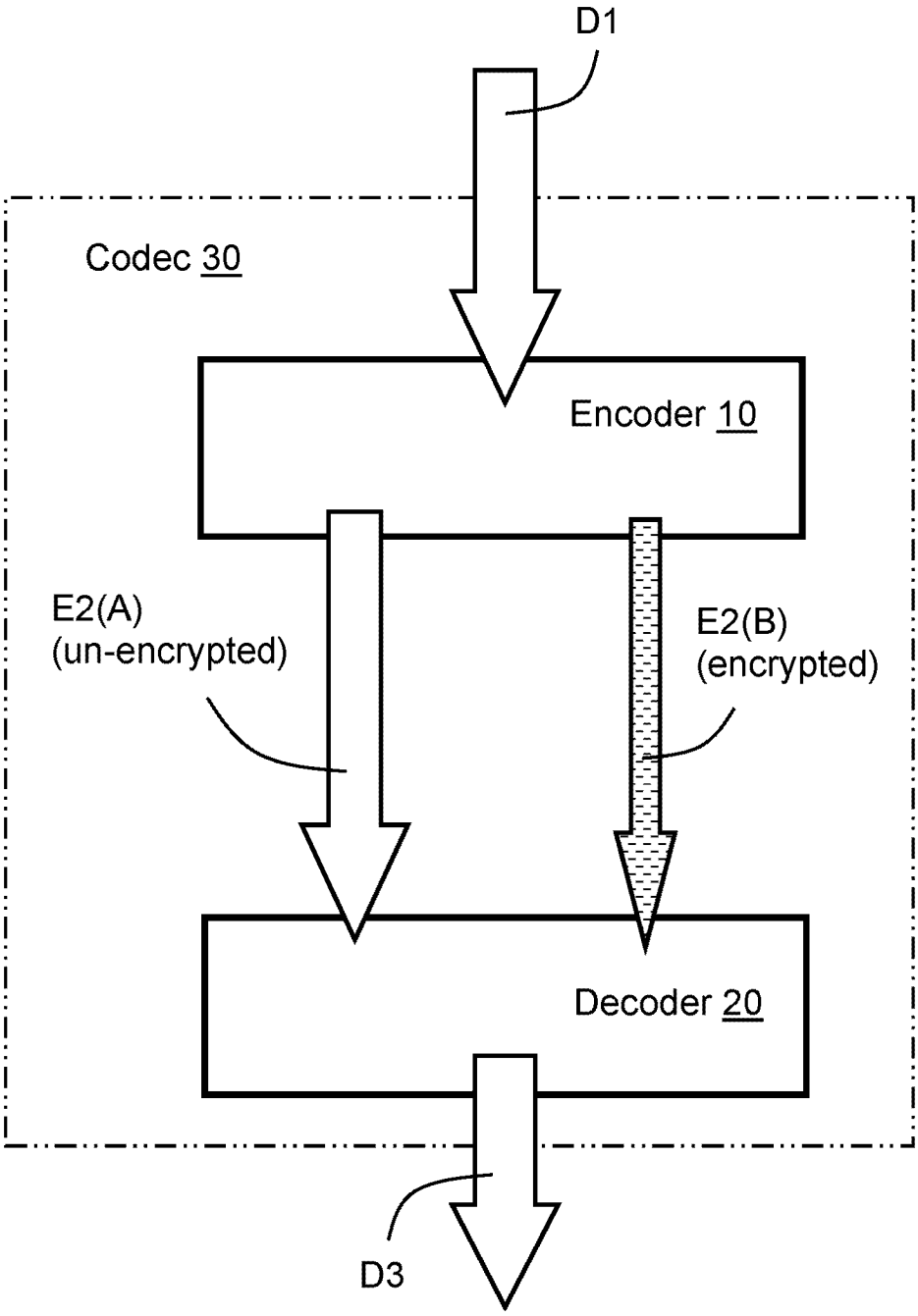
D1
Codec 30
Encoder 10
E2(A)
(un-encrypted)
E2(B)
(encrypted)
Decoder 20
D3

FIG. 1

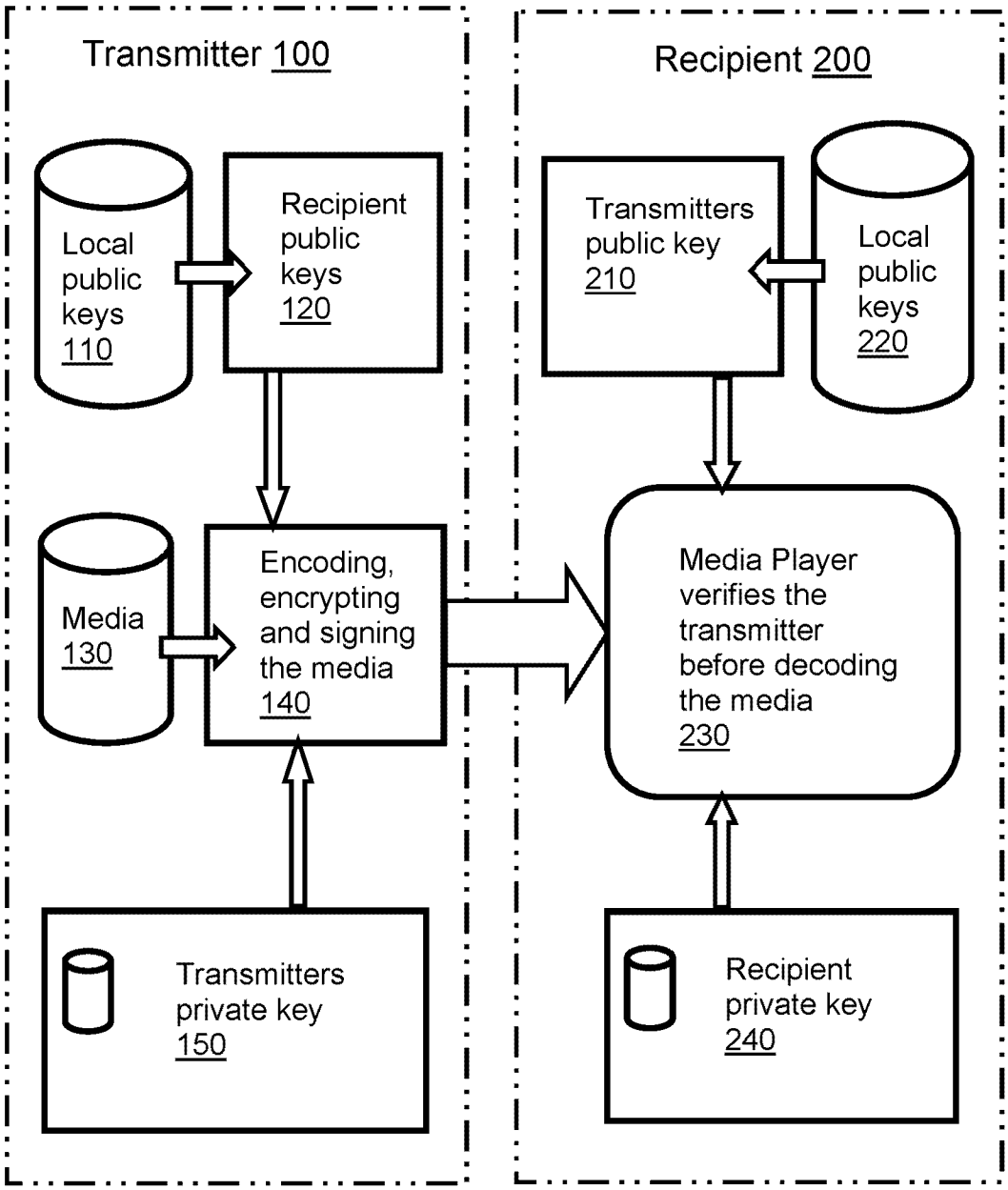
Transmitter 100
Recipient 200
Local public keys 110
Recipient public keys 120
Transmitters public key 210
Local public keys 220
Media 130
Encoding, encrypting and signing the media 140
Media Player verifies the transmitter before decoding the media 230
Transmitters private key 150
Recipient private key 240

FIG. 2

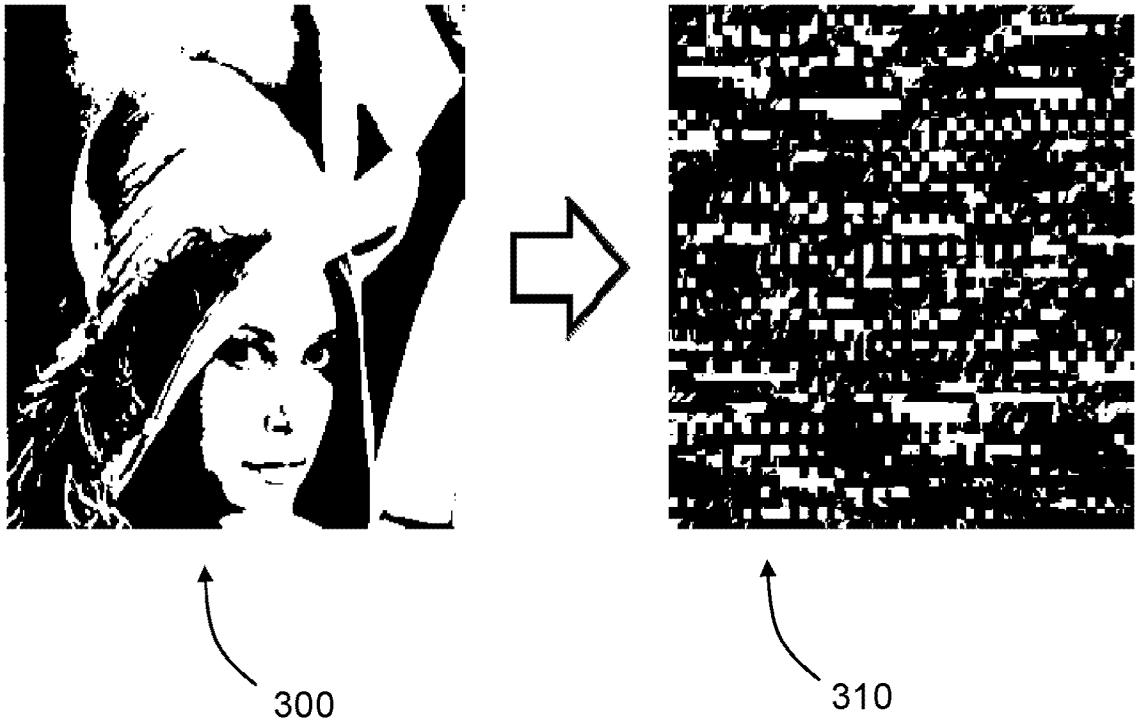

FIG. 3

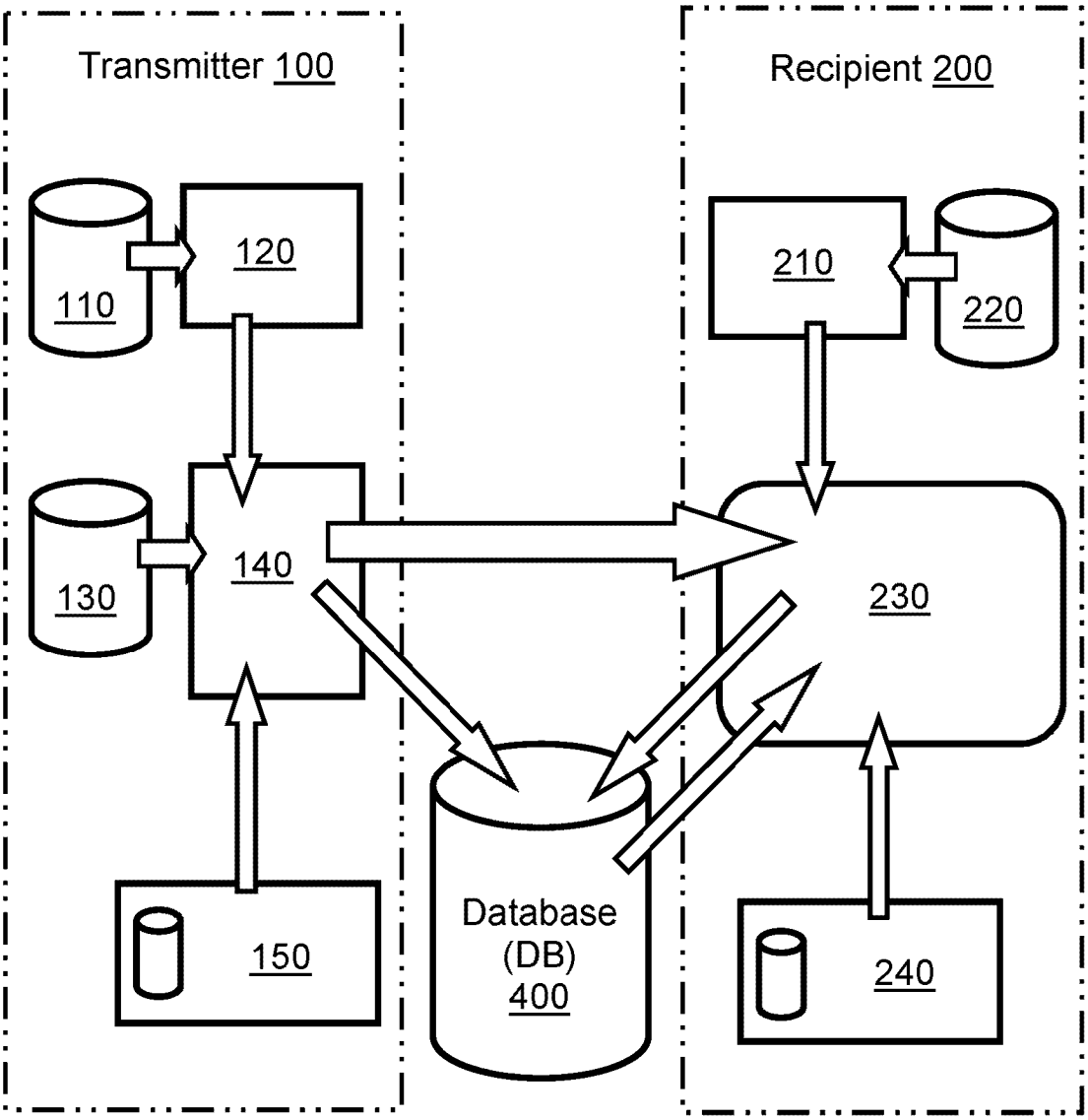
Transmitter 100
Recipient 200
120
110
210
220
140
130
230
Database
(DB)
400
150
240

FIG. 4

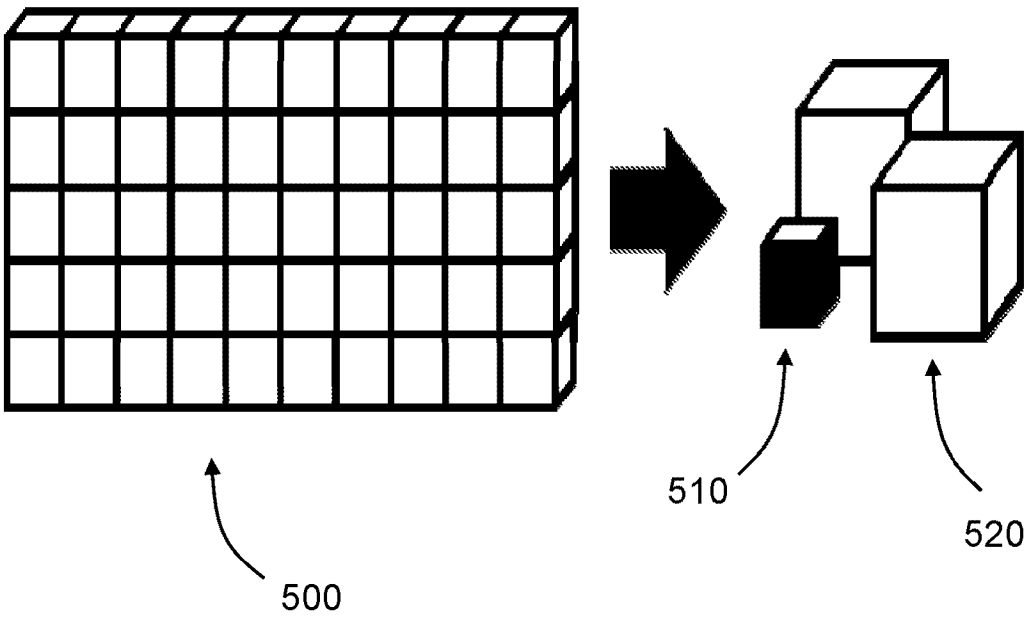

FIG. 5

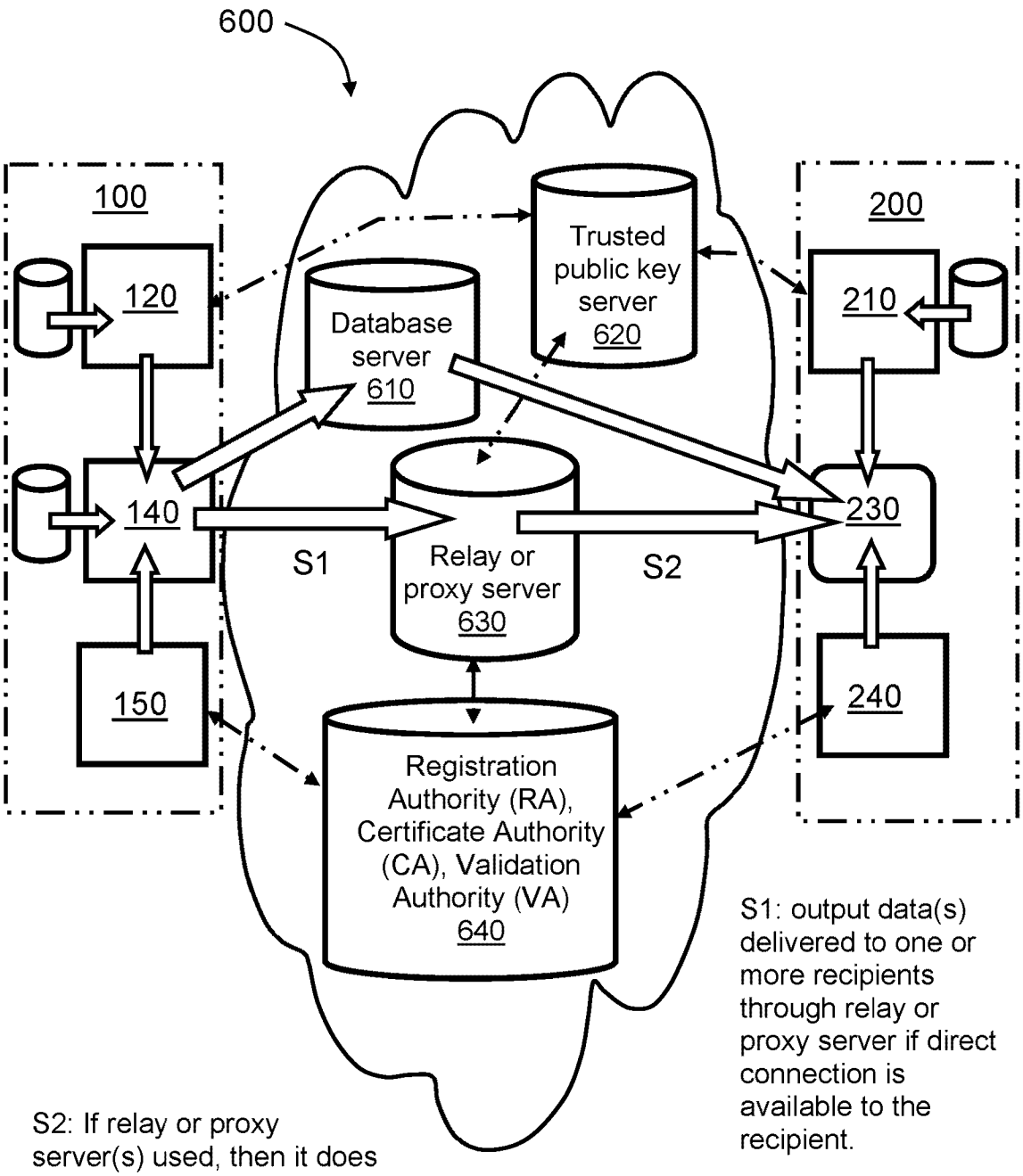
600
100
120
140
150
Database server 610
Trusted public key server 620
Relay or proxy server 630
Registration Authority (RA), Certificate Authority (CA), Validation Authority (VA) 640
200
210
230
240
S1
S2
S1: output data(s) delivered to one or more recipients through relay or proxy server if direct connection is available to the recipient.
S2: If relay or proxy server(s) used, then it does not cache any information, but possibly validates the transmitter's signature and validates the recipient(s), before redirection.

FIG. 6

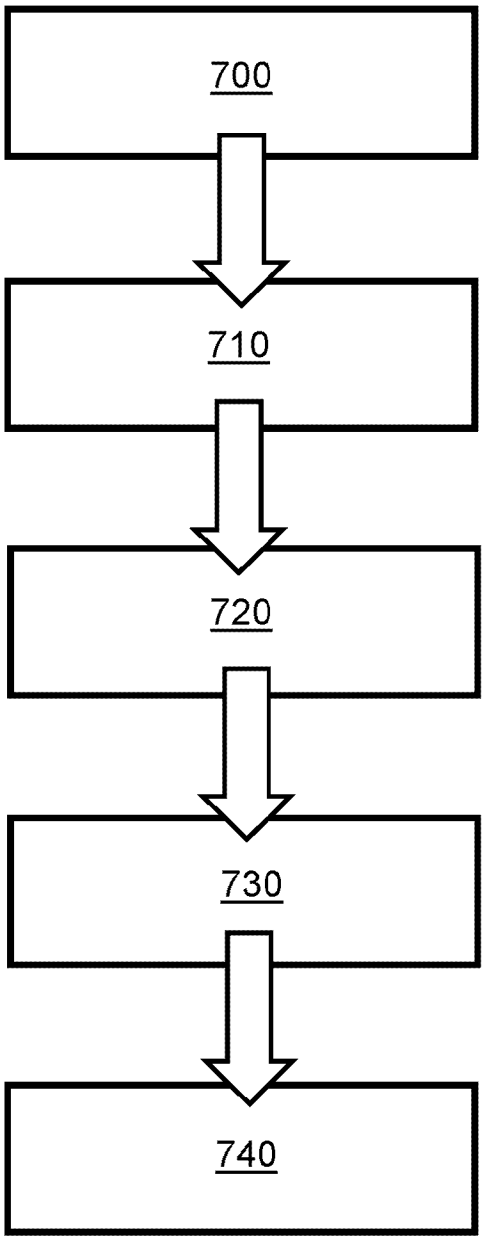

FIG. 7

The following terms are registered trade marks and should be read as such wherever they occur in this document:

YouTube

SECURE MEDIA PLAYER

Technical Field

The present disclosure relates to secure media players, methods of operating the secure media players, systems including the secure media players and also methods of operating the systems. Moreover, the present disclosure is concerned with computer program products comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute aforesaid methods.

Background

Various different content producers operate in connection with the contemporary Internet, such as cinema production companies in Hollywood. Moreover, private citizens produce all sorts of media content via use of YouTube and other social media sites and applications. Furthermore, several service providers operate in the Internet to offer their clients movies and TV series, or even live content via use of direct streaming. Additionally, globally, there are various different security implementations in use which attempt to implement protection, for example for military or commercial purposes, for example for governments, corporations, associations and other organizations, and also for consumers.

If a given consumer uses a given media content product without paying, it is usually a producer of the given media content who suffers commercial losses. Media companies have sued private citizens and groups of citizens and organizations for distributing illegal copies of media content that was copyright-protected. A recent example of such a legal trial relates to "*The Pirate Bay*" trial, wherein individuals who maintained an Internet website and associated service were sentenced to prison and to pay fines to copyright organizations and to media corporations.

In known technology, encryption techniques have often been implemented in such a way that media content information has been produced in an unencrypted format, and

the media content information is encrypted just prior to transmitting it, either by using an encrypted connection or by encrypting the media content information itself. The former approach of encryption just prior to transmission often encounters a problem that even though a given used transfer channel were secure, for example HTTPS or SSH, a given recipient still stores the media content information itself in unencrypted format at his or her media content device, thus making it possible to leak the media content information into wrong hands. However, such an encrypted transfer connection does enable a real-time online service to be offered to users, because the encryption is executed on the connection, and not on the media content information itself.

It can be assumed that various ways for encrypting information have been developed along with the development of reading and writing, and encryption techniques have been used since the times of Classical Antiquity, especially for military purposes. However, it is especially because computers and information networks became more and more common during the twentieth century that innumerous models for encrypting information have been produced. The most widely known of these is the RSA (see reference [1]), which was the first encryption technique that used public keys. It was considered very strong and it gave the impression of being an unbreakable.

Later on, as information technology has become more commonplace even among normal businesses and private citizens, on the basis of RSA, PGP (Pretty Good Privacy, see reference [2]) has been developed which is very well suited for encrypting both e-mails and hard drives of computing devices which are capable of storing media content information. A person of ordinary technical skill knows that a process of encrypting information operates in such a way that either a given entire information sequence, or a part of the information sequence, is encrypted so that only authorized parties are able to read it. Such encryption converts plain text information into encrypted information by using an encryption key, so that the encrypted information can be read, namely “opened”, only if the encryption information is decrypted with a right key which a given encrypting party has given to a recipient of the encrypted information. It is also well-known that it is in theory possible to break encrypted information, without having access to an encryption key used to generate the encrypted information, but such decryption without use of an encryption key would require so much computing capacity that it has not so far been possible to implement

in practice, other than with such gigantic resources that only certain intelligence agencies possess.

However, nowadays, it is also possible to encrypt entire media content information, which enables offering an offline service, namely the media content information is encrypted for certain recipients. Such an approach does not however make it possible to provide as cost-effective a solution pursuant to the present disclosure, because known approaches involve using considerable computer processing time and energy. Moreover, such considerable computer processing time is to be taken into account, especially in server arrangements where, for example, movies are transmitted in real time, because the solution pursuant to the present disclosure makes it possible to serve several client terminals simultaneously, yet using only a fraction of computing resources compared to known approaches where a whole given movie were encrypted, for each recipient separately.

Thus, the present disclosure seeks to provide an at least partial solution which makes it possible to distribute and render media content information safely as regards needs of content information owners. As aforementioned, it is one of the worst problems for media content information producers and media content information owners that they cannot be sure whether or not their produced media content information will at some point end up in wrong hands or to a public file sharing site. Media content information produced for commercial purposes has always had production costs associated therewith, and it is always customers, usually a consumer, who pays for these costs.

In a published WIPO patent application WO 2014/175910 A1 ("*Protected media decoding using a secure operating system*"; inventors: Glenn F. Evans, Shyam Sadhwani and Yongjun Wu), there are described tools and techniques for facilitating decoding of protected media information using a secure operating system. According to one exemplary technique, encoded media information that is encrypted is received at a secure process of a secure operating system of a computing system. At least a portion of the encoded media information that is encrypted is decrypted in the secure process. The portion of the encoded media information includes header information. Additionally, the header information is sent from the secure operating system to a software decoder for controling decoding hardware. The software decoder is included

in a process for an application. Moreover, the decoding hardware is securely provided access to the encoded media information for decoding the encoded media information to produce corresponding decoded media information.

In another published US patent application US 2004/0236940 A1 ("*Contents supplying system, method and program*"; inventor: Ryosuke Asai), there is described a method, wherein the method includes dividing contents to be supplied to a user divided into a core portion and one or more non-core portions, and appliying an encryption process to the core portion which is supplied to the user. Since the significant portion of the contents is used as the core portion, which is encrypted and transmitted, a whole the contents can be substantially protected by the encryption process of only the core portion.

In yet another published EP patent application EP 2346246 A1 ("*Contents supplying system, method and program*"; inventors: Robert Allan Unger, Brant L. Candelore), there is described an encryption arrangement for use when executing multiple encryptions of television programs. In implementations of a system described, multiple encryptions of only a portion of given data are required for full presentation of a corresponding television program to permit multiple manufacturers' set-top boxes within a single system to access the television program. In one embodiment of the system, only critical packets such as those carrying a payload incorporating packetized elementary stream header information is encrypted. By only encrypting a portion of the television program, dramatically less bandwidth is consumed than an alternative of multiple encryption of all data program of the television program, thus permitting a larger number of multiple conditional access systems in a single cable television system.

In still another published EP patent application EP 2073545 A2 ("*Video processing system for scrambling video streams with dependent portions and methods for use therewith*"; inventors: Sherman Chen (Xuemin), Michael Dove, Stephen E. Gordon, Jeyhan Karaoguz, Thomas J. Quigley and David Rosmann), there is described a video processing system which includes a video encoder that encodes a video signal into a contiguous video stream having an independent portion and a dependent portion that requires the independent portion for decoding. A scrambling module scrambles the

contiguous video stream to produce a scrambled video stream by scrambling the independent video portion and leaving the dependent portion unscrambled.

In yet another published WIPO patent application WO 2010/042318 ("*Method and system for encrypting and decrypting data streams*"; inventors: Richard Greene, Igor Komir and Ronnin Yee), there is described a method of encrypting a data stream which includes receiving the data stream, and for each data packet in the data stream, forming an encrypted packet by encrypting a header portion of the data packet while leaving a body portion of the data packet unencrypted. The method also includes assembling an encrypted data stream comprising all the encrypted packets, and outputting the encrypted data stream.

In yet another published US patent application US 2003/0152226 ("*Slice mask and moat pattern partial encryption*"; inventors: Brant Candelore, Henry Derovanessian and Leo Pedlow), there is described a selective encryption encoder for use in implementations described in the patent application, wherein the selective encryption includes arranging for vertical and/or horizontal stripes of data to be encrypted. In one implementation, packets are examined in a digital video signal to identify a specified packet type, wherein the specified packet type concerns packets carrying intra-coded data representing a pattern of horizontal stripes across an image and packets carrying intra-coded data representing a pattern of vertical stripes across an image. The packets identified as being of the specified packet type are encrypted using a first encryption method to produce first encrypted packets. These first encrypted packets are then used to replace the unencrypted packets in the digital video signal to produce a partially encrypted video signal. The packets of the specified type can also be encrypted in a plurality of ways and replaced in the data stream to produce a multiple encrypted video data stream.

Summary

The present disclosure seeks to provide an improved secure media player which is operable to communicate and render media content information in a more secure and efficient manner.

Moreover, the present disclosure seeks to provide an improved method, in a secure media player, of communicating and rendering media content information in a more secure and efficient manner.

According to a first aspect of the present invention, there is provided a secure media player system for communicating media content information (D1) from an encoder to at least one decoder, wherein the encoder is operable:

(a) to process and encode the media content information (D1) into one or more first sections of data (E2(A)) and one or more second sections of data (E2(B)), wherein the one or more second sections of data (E2(B)) include one or more parameters which enable the media content information (D1) to be regenerated from the one or more first sections of data (E2(A));

(b) to encrypt the one or more second sections of data (E2(B)) to generate corresponding one or more encrypted second sections of data (encrypt(E2(B)));

and

(c) to communicate the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))) to the at least one decoder for the at least one decoder to process and render the media content information (D3) to one or more users,

characterized in that the secure media player system does not store or allow the at least one decoder (20, 200) to store the one or more encrypted second sections of data (*encrypt*(E2(B))) in an unencrypted form into a memory from which the one or more second sections of data (E2(B)) can later be downloaded in an unencrypted manner, wherein the secure media player system stores at the at least one decoder (20, 200) the one or more encrypted second sections of data (*encrypt*(E2(B))) in an encrypted form.

The present invention is of advantage in that generating the first and second sections of data enables a reduced amount of data encryption to be utilized, and a greater portion of the media content information conveyed from the encoder to the at least one decoder in merely an encoded form, without a need for encryption to be employed.

Optionally, the secure media player system is implemented, such that the one or more encrypted second sections of data (*encrypt(*E2(B))) are encrypted using at least one encryption key that identifies the encoder when the at least one decoder processes the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))).

Optionally, the secure media player system is implemented, such that the at least one decoder is provided with a complementary key to that used by the encoder when generating one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))), wherein the complementary key is used by the decoder to process and render the media content information (D3) to the one or more users.

More optionally, the secure media player system is implemented, such that the one or more keys are provided from at least one of: a validating authority, a certifying authority, a verification authority.

Optionally, the secure media player system is implemented, such that the system is operable to customize uniquely the one or more encrypted second sections of data (*encrypt(*E2(B))) for each corresponding decoder.

Optionally, the secure media player system is implemented, such that at least the one or more first sections of encoded data (E2(A)) are communicated via at least one relay and/or proxy server which is operable to service a plurality of decoders with the encoded data (E2(A)).

According to a second aspect, there is provided a method of communicating media content information (D1) from an encoder to at least one decoder within a secure media player system, wherein the method includes:

(a) processing and encoding the media content information (D1) into one or more first sections of data (E2(A)) and one or more second sections of data (E2(B)), wherein the one or more second sections of data (E2(B)) include one or more parameters which enable the media content information (D1) to be regenerated from the one or more first sections of data (E2(A));

(b) encrypting the one or more second sections of data (E2(B)) to generate corresponding one or more encrypted second sections of data (encrypt(E2(B)));
and

(c) communicating the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))) to the at least one decoder for the at least one decoder to process and render the media content information (D3) to one or more users,

characterized in that the secure media player system does not store or allow the at least one decoder (20, 200) to store the one or more encrypted second sections of data (*encrypt*(E2(B))) in an unencrypted form into a memory from which the one or more second sections of data (E2(B)) can later be downloaded in an unencrypted manner, wherein the secure media player system stores at the at least one decoder (20, 200) the one or more encrypted second sections of data (*encrypt*(E2(B))) in an encrypted form.

Optionally, in the method, the one or more encrypted second sections of data (*encrypt(*E2(B))) are encrypted using at least one encryption key that identifies the encoder when the at least one decoder processes the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))).

Optionally, in the method, the at least one decoder is provided with a complementary key to that used by the encoder when generating one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))), wherein the complementary key is used by the decoder to process and render the media content information (D3) to the one or more users.

More optionally, in the method, the one or more keys are provided from at least one of: a validating authority, a certifying authority, a verification authority.

Optionally, the method includes customizing uniquely the one or more encrypted second sections of data (*encrypt(*E2(B))) for each corresponding decoder.

Optionally, in the method, at least the one or more first sections of encoded data (E2(A)) are communicated via at least one relay and/or proxy server which is operable to service a plurality of decoders with the encoded data (E2(A)).

According to a third aspect, there is provided a computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the aforementioned method pursuant to the fifth aspect.

It will be appreciated that features of the invention are susceptible to being combined in various combinations without departing from the scope of the invention as defined by the appended claims.

Description of the diagrams

Embodiments of the present invention will now be described, by way of example only, with reference to the following diagrams wherein:

FIG. 1 is a schematic illustration of a system for distributing media content information in a secure manner pursuant to embodiments of the present disclosure;

FIG. 2 is an illustration of features of a Secure Media Player pursuant to an embodiment of the present disclosure;

FIG. 3 is an illustration of an image, for example present in media content information D1, and a visualization of a first section of data E2(A) conveying components present in the information D1, but without being decoded with respect to a second section of data E2(B) generated from the information (D1) during encoding in an encoder, for example included as a part of a transmitter;

FIG. 4 is an illustration of features of the Secure Media Player of FIG. 2, employing a database (DB) arrangement;

FIG. 5 is an illustration of decompressing a size of the original media content information pursuant to an embodiment of the present disclosure;

FIG. 6 is an illustration of an implementation of an embodiment of the present disclosure based on public key infrastructure; and

FIG. 7 is an illustration of a method of encoding and decoding data pursuant to the present disclosure.

In the accompanying diagrams, an underlined number is employed to represent an item over which the underlined number is positioned or an item to which the underlined number is adjacent. A non-underlined number relates to an item identified by a line linking the non-underlined number to the item. When a number is non-underlined and accompanied by an associated arrow, the non-underlined number is used to identify a general item at which the arrow is pointing.

Description of embodiments

In overview, embodiments described in this disclosure are based on distributing and encryption of information and on authenticating both a given transmitter of the encrypted information, and one or more receivers of the encrypted information via use of at least one digital signature verified by a Validation Authority (VA), thereby ensuring authentication of all parties and a reliable communication of the encrypted information.

An example implementation of embodiments of the present disclosure is a Gurulogic® Media Player; this Media Player, namely "*Secure Media Player*", makes it possible to verify the authenticity of a recipient in such a way that content can be played only by such recipients for whom it was meant. Moreover, Gurulogic® Media Player is a safe concept for media content information producers, media content information distributors and media content information owners. Technology described in this disclosure therefore implements a form of verification of authenticity and protection against unauthorized copying for renderable media content information or for other types of information. Optionally, it is possible to verify also the media content information for example for the purposes of checking that the security classifications of the transmitter are fulfilled (i.e. the transmitter is allowed to send the information) or of the recipient (i.e. the recipient is allowed to see the information).

Embodiments of the present disclosure also concern a method that keeps at least part of the media content information encrypted all the time and only the Secure Media Player is operable to open the media content information for use. Moreover, the Secure Media Player does not store or allow others to store the media content information in

an unencrypted form. Furthermore, the Secure Media Server is able to do encryption transcoding that changes the media content information encrypted for a given server, so that the media content information is encrypted for the recipient. Optionally, national security operators can open the media content information, similarly like the Secure Media Server, and this means that, for example, authorities in the USA are able to open all content that is in their Secure Media Server, but not content that is, for example, in a China Secure Media Server, and vice versa. When multiple keys for multiple states are used then states have to co-operate, if they want to open, namely decrypt, that kind of information. Any state alone can't decrypt the information. There is a variety of different methods to use multiple keys. The key might be combination of multiple keys, the keys can be used one after another to the same data, or different parts of the data might be encrypted with different keys, etc.

The secure transmission of media content information described for embodiments of the present disclosure provides media content information producers, media content information distributors and also end users an opportunity to validate all parties involved in a corresponding media content information transfer chain, while simultaneously securing the media content information being transmitted in a very cost-effective way, so that security will not be compromised, thereby enabling a secure commercial implementation of various different media content information services. Therefore, the technology described in this disclosure is useable to create a safer and more secure data distribution network, for example a safer Internet.

In embodiments of the present disclosure, only the critical information of data content to be distributed is encrypted, such that, for example, 90 % of the data content can be freely available for use of everybody, but this critical information, for example 10 % of the data content that allows Secure Media Player to understand the data content, is encrypted for each recipient separately. Such encryption transcoding of critical information is then a relatively light data processing operation, and the Secure Media Server enables very efficient data distribution solution for, for example, online video services to be realized.

Therefore, in server solutions such as aforementioned pursuant to the present disclosure, stream content to several clients simultaneously is achievable in real time,

the distributed information encryption described in this disclosure is useable and thereby saves on energy spent in encryption, or uses the energy more efficiently. It will be appreciated that, in embodiments of the present disclosure, the content is beneficially encrypted for each recipient separately, but still only small fraction of the data is delivered separately for each recipient and big fraction of the data can be delivered for all recipients similarly. It is for that reason that embodiments of the present disclosure include a method for encrypting the information content itself, so that a given used transfer channel will not compromise security, even though the information were transmitted in the public Internet which enables running both an online service and an offline service simultaneously.

In principle, a majority of media content information can be transmitted in a known traditional manner by using either an unencrypted connection protocol, such as HTTP, or an encrypted one, such as HTTPS, but a most essential reason for encrypting information and to use digital signatures pursuant to embodiments of the present disclosure is to ensure the authenticity of the recipient to the transmitter, namely to detect to whom the requested information is transferred. Correspondingly, a given recipient needs to be able to know, and optionally verify, the authenticity of the transmitter. Thereby, unauthorized viewing and manipulation of media content information is prevented.

Technology described in the present disclosure is possible to implement in other ways as well, but the present disclosure provides a least one model for a public key infrastructure (PKI), adapted for the needs dictated by a usage scenario associated with the present disclosure, namely to try to guarantee secure rendering and storing of media content information. The media content information is stored, it is possible for the transmitter to make it expire after a period of time, after which the information can no longer be decrypted if it has expired. Such a functionality enables a control mechanism for accessing the transmitted media content information. The aforementioned Secure Media Player is also able to validate when the media content information is valid, for example by using a world clock.

In an event that a need arises later to render the media content information again, the media content information in question is beneficially requested again from the

transmitter, in which case only the encrypted part of the entire media content information is transmitted, which is only a fraction of the entire media content information. However, it will be appreciated that the recipient needs to have the rest of the expired media content information still stored locally, or else it is beneficially re-downloadable from, for example, a proxy server. Therefore, the transmitter needs to keep record of whether the media content information is available for online purposes or for offline purposes, and to define an expiry date of the encrypted media content information accordingly.

Regardless of whether a given system for media content information pursuant to the present disclosure is running in an offline mode or an online mode, the user needs to execute an initialization procedures, wherein the user must have his or her own digital certificate, the creation of which the Secure Media Player will assist when necessary. Optionally, an existing certificate is used.

When the user requires to obtain a digital certificate, he or she sends an application for a digital certificate to a PKI Certification Authority (CA), for example to a CA-server of Gurulogic Microsystems Oy or Verisign, that verifies the authenticity of the user at a PKI Registration Authority (RA), for example at a bank or a national Social Security Administration. Using CA and RA in combination for purposes of authentication and verification ensures that a reliable authentication mechanism is employed in embodiments of the present disclosure. In such a manner, a public key and a certificate are bound to, namely associated with, a legal personality. Optionally, the user already has a suitable certificate, in which case that suitable certificate is used, but the authenticity of the user still needs to be verified at a PKI RA. For example, if the RA is a bank, an existing authentication system for secure online banking is optionally used to verify an authenticity of a legal personality.

The PKI, CA or the Secure Media Player transmits the public key of the user to a certified key server, for example to a public key server of Gurulogic Microsystems Oy. Such an initialization procedure for PKI as described above is required of each user, regardless of whether the user is a transmitter (encoder) or a recipient (decoder).

After authenticating the user, it is possible to commence transmitting protected media content information, in such a way that either the entire media content information, or a part thereof, is encoded and encrypted, or else already partially or entirely encoded media content information is encrypted, by using a public key of the recipient and a private key of the transmitter. To save on computing resources, the media content information is optionally encrypted by using a symmetric-key cryptography method, such as AES, for which the used encryption key is produced by a pseudo-random method such as HMAC, and then the created key is encrypted by utilizing an asymmetric public key encryption method such as RSA. Partial media content information is optionally also encrypted only via utilization of a public key encryption method such as RSA. The encryption of the media content information is optionally also executed using various different combinations of encryption methods, according to usage needs. In the foregoing, it will be appreciated that "*media content information*" includes potentially a broad range of content, for example generated or measured content at least one of: numerical data, text data, image data, video data, seismic data, audio data, but not limited thereto.

By using procedures as described above, reliable, secure and authenticated media content information distribution is beneficially targeted per user, individually, either via utilizing online data transfer mechanisms or offline data transfer mechanisms. Normally, in known methods, the encryption of the media content information is executed on the entire content information, but embodiments of the present disclosure beneficially utilize a partial encryption of media content information in such way that the information is transmitted in two sections, wherein a first section contains a majority of the information and which is transmitted unencrypted, and a second section which includes a sequence which is encrypted. The two sections are optionally delivered temporally to a given user in any order; moreover, the sections are optionally in data fragments or data slices, depending upon a nature of a data transmission route employed to deliver the sections to the given user. The encrypted sequence contains such information which is essential for the media content information, for example including split and method selection information, headers, stream flags and so forth; without access to information in the encrypted sequence, for example an image or a video delivered to the given user would be just static, for example as illustrated in FIG. 3. Optionally, the encrypted sequence contains information on the used database such

as database references and/or database delivery location and the selected database(s), for example as illustrated in FIG. 4, without which the media content information data cannot be decompressed.

This partial encryption of media content information, pursuant to embodiments of the present disclosure, enables a very efficient way to transmit safely the essential information for decompressing the media content information. This essential information is easy to re-encrypt, even for more than one recipient, if necessary.

There is thus provided in the foregoing a novel and inventive method of transmitting media content information, such as images and video, for example as useable in an advanced form of codec. Encryption of the media content information is beneficially executed not only for a recipient but also for the transmitter itself or even for a third party, if legislation of a given country in question requires that, for example pursuant to US legislation. For example, authorities of a given target country always have an opportunity the decrypt the encrypted section and to assemble the entire content using that, as do each recipient, without wasting resources, thereby saving on precious energy and preserving nature and preventing criminal activity.

Referring to FIG. 1, there is shown an illustration of an embodiment of the present disclosure. In FIG. 1, encoder **10**, for example associated with a transmitter, is operable to receive media content information represented by data D1 and to encode and/or encrypt the data D1 to generate a first un-encrypted section of data E2(A) and a second encrypted section of data E2(B). The sections of data E2(A), E2(B) are communicated to one or more decoders **20**, for example associated with one or more recipients, wherein the one or more decoders **20** are operable to decrypt the second section of data E2(B) to generate corresponding decoded data which is used to process the first section of data E2(A) at the one or more decoders **20** to generate output data D3. Encryption and decryption at the encoder **10** and the decoder **20** is optionally subject to use of various keys as will be elucidated in greater detail later. Supply of the keys is dependent upon authentication and validation of parties associated with the encoder **10** and the one or more decoders **20**. Optionally, the keys are time-limited as will be described in more detail later. Optionally, the data D1 corresponds to an image indicated generally by **300** in FIG. 3, and the first section of

data E2(A), if eavesdropped by an unauthorized third party, would appear as indicated generally by **310** in FIG. 3. Beneficially, the encoder **10** and the decoder **20** in combination form a codec denoted by **30**.

Thus, the recipient decrypts the encrypted part, namely the second section of data E2(B), of the entire media content information and assembles the first and second sections of data E2(A) and E2(B) into an entirety, represented by the output data D3, the encoding of which is beneficially decompressed if the signature of the transmitter has been authenticated. The signature of the transmitter is beneficially verified by a Validation Authority (VA), if that has not already been done. It is also possible to verify the authenticity every time, but in practice, the verification is executed by marking a public key of the transmitter as read, in which case it is stored in a system including the encoder **10** and the one or more decoders **20**, but only for a limited period, depending on the expiration date of the certificate. Despite this, the system must regularly validate the authenticity of the digital certificate at the VA in case the certificate authority has declared the certificate invalid, for example because its confidentiality was compromised.

The rendering of the media content information at the decoder **20**, for example via audio replay and/or image display apparatus associated with the decoder **20**, is beneficially started when the entire media content information has been at least partly decompressed into data memory associated with the decoder **20**, but care is beneficially taken not to store the decompressed part into such a RAM/ROM memory which can later be downloaded in an unencrypted manner. Such an example player of media content information also optionally reinitialize all its used memories after the data D3 has been consumed to avoid residual data being in some data memory after consumption thereof, for example by way of user viewing the media content information. According to an embodiment of the present disclosure, the encryption integrated into the encoder **10,** as described in not yet public patent application GB 1414007.3 filed by the Applicant, is beneficially used, in which case the system decompresses encrypted information only a fraction at a time, which prevents someone from attempting to capture the decompressed information from the player. However, such an approach does not prevent a third party merely making a video recording and/or audio recording of the media content information rendered to a given

user, albeit often of somewhat inferior quality; this is achieved by making a video, for example, of a display screen of a rendering device.

Procedures described above prevent entire copying of media content information, at least in its original quality, because as a counterpart to the encryption integrated into the encoder **10** described above, the decryption of encrypted content is integrated into the decoder **20**, which prevents copying of information. Therefore, Gurulogic Microsystems has developed technologies, for example as described in a granted patent US 8,675,731 B2 ("*Encoder and method*", ref. GURU004US), patent application EP 13002520.8 ("*Decoder and method*", ref. GURU005EP), patent application GB 1416631.8 ("*Encoder, Decoder and Methods employing partial encryption*"), and GB 1414007.3, ("*Encoder, Decoder and Methods*") which are susceptible to being implemented precisely as described above. It is also possible to use other technologies and other codecs, as long as the Secure Media Player and optionally Secure Media Server solutions are used.

As aforementioned, nothing prevents a user to directly copy the media content from the display by using a video camera, but in that case it will no longer be authentic media, namely lossless. Moreover, techniques exist with which the video being rendered can be captured simply by installing a virtual video card into a computer, but a risk of getting caught limits the number of perpetrators, because each authenticated user has been verified according to the jurisprudence of the target country. Optionally, watermarking is added to the media content information when decoded to generate the decrypted data D3, wherein the watermarking is implemented to be unique for each recipient. The watermarking is implemented, for example by imposing a constant faint watermarking image over region of static image information present in the media content information represented by the data D1.

This means that the perpetrators will have to think twice before starting to commit a copyright infringement. Moreover, in the system described above, as each party has been authenticated, it is made possible to distribute in the media content information, such example audio-visual information that is targeted precisely for an individual user, for the one that it was originally sent to. Therefore, if the user had copied the content with a video camera and then given that copyright-protected material into public

distribution, it would be possible to find out who the perpetrator was and to hold that person legally accountable for his or her actions. Such targeting includes, for example, a combination of a plurality of user-unique advertisements which are added discreetly to images of the media content information.

Each Secure Media Player beneficially also attempts to prevent video window screen captures by using video overlay in the window, in which case the operating system cannot capture or analyze the video image rendered on the screen. Moreover, the Secure Media Player can be set to be allowed to operate only in a limited set of accepted device configurations, depending on the signature of the media content information.

As illustrated in FIG 2, the media content information, represented by the data D1 in FIG. 1, is beneficially encoded in its entirety, but only an essential fraction of it is encrypted, namely the section of data E2(B). For encoding the media content information, for example a proprietary GMVC® codec is used, which yields a cost-effective compression ratio and simultaneously encapsulates various different pieces of information of the media content information, from among which essential sequences of information can then be selected that will be encrypted using, for example, a public key infrastructure.

In FIG. 2, there is shown an illustration of component parts associated with a transmitter **100** and a recipient **200** of an embodiment of the present disclosure. The transmitter **100** includes the encoder **10**, and the recipient includes the decoder **20**. There is optionally a plurality of recipients **200** connected to a transmitter **100**, forming a system pursuant to the present disclosure.

The transmitter **100** includes access to a database **110** of local public keys **110** for providing recipient public keys **120**. Moreover, the transmitter **100** includes access to media content information from a media database **130**. Furthermore, the transmitter **100** includes access to the transmitter's private keys, denoted by **150**. The transmitter **100** also includes an encoding arrangement **140**, for example including the encoder **10**, for encoding, encrypting and signing media content information provided to the encoding arrangement **140** from the media database **130**.

The recipient **200** includes access to a local public key database **220** for providing the transmitter's public key **210**. Moreover, the recipient **200** includes access to a database **240** for providing the recipient's private key. Furthermore, the recipient **200** includes a decoding arrangement **230**, for example including the decoder **20**, which is operable to verify the transmitter **100** before commencing to decode the data E2(A) and E2(B) received thereat for generating corresponding output data D3, as described in the foregoing.

A manner in which the system pursuant to the present disclosure functions is described in overview, but at its simplest, the transmitter **100** must encrypt desired pieces of information by using his or her private key, against the public keys of the recipients **200**. Thereby, a majority of the media content information, namely the data D1, is beneficially transferred in an unencrypted manner, which enables a very fast and reliable technique for transferring encrypted media content information to be achieved in operation in the system, whereby the transmitter **100** makes sure who will receive the data E2(A) and E2(B), and correspondingly, the recipient **200** is ensured that the transmitter's origins are authentic. It will be appreciated that the unencrypted information to be transmitted, namely the data E2(A), is optionally sent together with the encrypted content, namely the data E2(B), or they can be sent separately, namely the data E2(A) is sent via a different route to that employed to send the data E2(B). The two sections are optionally delivered temporally to a given user in any order; moreover, the sections are optionally in data fragments or data slices, depending upon a nature of a data transmission route employed to deliver the sections to the given user.

In FIG. 3, there is shown an illustration of a depiction of how a decoded image looks like when an attempt has been made to decompress the image without the tiny little fraction E2(B) of the encoded media content information which simply defines where the blocks are situated and what their sizes are, for example. This kind of result can be seen with human eyes. If more information were to be encrypted, then it would be very probable that a media decompressor would not be able to finish the image, because the code would contain too many syntax errors. Designing this example alone requires a lot of sophisticated knowledge on how a video decoding process operates,

for example as employed in the aforementioned GMVC® codec. However, this example demonstrates that the majority of encoded media content information can be transmitted unencrypted, via the section of data E2(A), and over an unencrypted transfer channel, but without the tiny little piece of encrypted vital information, namely the section of data E2(B), the rest of the media content is unusable.

In an embodiment illustrated in FIG. 4, the media content information D1 is encoded in its entirety, but only those pieces of information are encrypted, namely in the section of data E2(B), which have been selected to be downloaded from a central database (DB) **400**. In this case, any information referring to the database **400** needs to be encrypted and to be transmitted in encrypted format, among the rest of the encoded information or separately. Thereby, the database references define all the rest of the information that is necessary for decompressing and rendering the encoded media content E2(A) and E2(B). It will be appreciated that the database depicted in FIG. 4 (DB) can simultaneously function as an authenticity controller, namely as a validation authority (VA), for the transmitter **100**, for the recipient **200** and also for the information itself.

If a piece of information referred to in the reference cannot be found in the database (DB) **400**, then this missing piece needs to be transmitted to the database **400** or to a centralized database. The database **400** can be local, namely mirrored from the centralized databases, but it can also be an external database that operates independently or that is connected with other databases, thereby constructing its own database system. The recipient **200** fetches the missing pieces of information for the centralized database, which makes it possible to render and store the media content information as explained above. More details on the usage of databases for employing the embodiment pursuant to the disclosure can be found in the database solution designed and patented by Gurulogic Microsystems Oy in GB 2509055 A.

In FIG. 5, there is an illustration of a size of the original media content information, namely the data D1 indicated generally by **500**, that is encoded into a much compressed size, indicated generally by **520**, and simultaneously the selected fraction of vital information, indicated by **510**, is encrypted, wherein this fraction is considerably

smaller than the entire encoded media content information, namely a combination of **510** and **520**. This way, the media content information can be both transmitted securely and cost-effectively and its authenticity can be verified. It will be appreciated that encryption algorithms require a lot of processing time and consume a lot of electricity and computing power. Therefore, the overall capacity of the system is saved to be used for other functionalities, especially in mobile devices that operate on battery power, and also in server farms, where the critical factor is energy consumption and not the computing capacity. It will also be appreciated that the information components present in the data **520** can relate to data blocks of mutually different sizes and that increases even more the security of the information content protection provided by the system of the disclosure.

Referring next to FIG. 6, there is shown an illustration of a public key infrastructure which is adapted for secure transmitting and rendering of media content information as described in the foregoing. It will be appreciated that the validation authority (VA) is optionally situated in the database server, namely the database **610**, if a database server is used. Moreover, FIG. 6 depicts the use of a relay server and a proxy server **630**, as a possible transmitter or as filter, depending on whether the transmitter **100** or the recipient **200** needs to comply with an information security policy that is used when communicating in a network in question.

Optionally, anti-virus software, a firewall or other data security related matter may require the use of relay servers or proxy servers as mentioned above. In principle, the secure transmitting of media content information described for embodiments of the present disclosure does not require that an encrypted connection be used between the transmitter **100** and the recipient **200**, even though it is advisable and yields additional protection and possibly prevents the attackers from abusing the vulnerabilities of information systems. It is beneficial to use a newest TLS-encrypted connection between the transmitter **100** and the recipient **200**, and also between all the other parties involved, but especially when communicating with Registration Authorities (RA), Certificate Authorities (CA) and Validation Authorities (VA).

In an embodiment described above, public key infrastructure is optionally used, which is known for several different vulnerabilities unless an encrypted connection is used

when communicating with the various authorities. It will be appreciated that the operation of a public key server must be protected in such a way that it is allowed to store only verified keys thereat, in which case malicious or undesired parties are prevented from posing as another recipient **200**.

It will be appreciated that the public key of a user will be transferred automatically to a public key server only in connection with the certification procedure. When the user adds verified public keys to his or her information system, it must be made sure that they are stored securely, correspondingly as the user's private key is stored as protected by the user's password for the computer in question. As regards data security, it is important to understand which is the weakest link of entirety of the encryption system, namely when and where the certificates of the terminal devices are stored and how strong encryption keys are used for encrypting the media content information D1. The encryption of the information D1 itself does not cause a security issue if mutually agreed security measures are obeyed, but it is usually the user himself or herself that causes the severest problems regarding data security. With the Secure Media Player solution pursuant to the disclosure, there is optionally additional security added also in situations where the private key is somehow been received by a third party. If the Secure Media Player solution has been implemented by employing a proprietary codec such as GMVC® and the control of the Secure Media Player(s) is made properly, there should not be any Secure Media Player provided by others available that can show the encrypted content even if the third party knows the private key. Even it is possible to open the encrypted content E2(A) and E2(B), there is still not suitable player available that can show the entire media content information D1.

Embodiments of the present disclosure are beneficially employed in combination with novel codec technologies described in a granted patent US 8,675,731 B2 ("*Encoder and method*", ref. GURU004US), patent application EP 13002520.8 ("*Decoder and method*", ref. GURU005EP), patent application GB 1416631.8 ("*Encoder, Decoder and Methods employing partial encryption*") and GB 1414007.3, ("*Encoder, Decoder and Methods*") that makes it possible to provide both stronger encryption keys than previously, and also a more secure way to transfer information between the transmitter **100** and the recipient **200**. Novel codec technologies includes encryption of information

in connection with encoding the information, which makes it possible to encrypt the information with a stronger encryption key than in prior art solutions, and also encrypting only a small part of the information. When this new method of encrypting information is integrated, for example, with the encoding of image or video information in such a way that only a fraction of the entire information sequence is encrypted, without which the decompression of the information is possible, regardless of used prediction methods, considerable gains are achieved as compared with known data communication arrangement, for example used for distributing media content information such as movies. Known data communication arrangements require that the entire telecommunications connection be encrypted, or entire content to be communicated.

For example, using the encryption method presented in this invention, before a movie is transmitted to a consumer, only certain important references and/or the database delivery information are encrypted, which are optionally downloaded from another server and which are vital for assembling and decompressing an entire video content of the movie. These references are only a fraction of the entire movie content, but without these selected parts of reference information, the rest of the video content becomes unusable, for example as illustrated in FIG. 3. To ensure a functional system, it is important not to select such pieces of information as references which would be easy to predict mathematically, such as the DC-components used in coding video images, which would be fairly easy to detect and thus would not guarantee secure operation.

Referring next to FIG. 7, steps **700** to **740** depict principal steps of methods employed in embodiments of the present disclosure.

In the encoder **10**, in the step **700**, the media content information D1 is received and the encoder **10** processes the media information content information to generate a first section of data E2(A), and a second section of data E2(B) (in unencrypted format), wherein the second section of data E2(B) provides one or more parameters which enable the media content information D1 to be regenerated from the first section of data E2(A). Generation of the sections of data E2(A), E2(B) require one or more encoding processes to be implemented in computing hardware of the encoder **10**.

In the encoder **10**, in the step **710**, the second section of data E2(B) is encrypted, for example using a private key of the encoder **10** and/or a public key of the recipient **20**. Optionally, these keys are time limited.

In the step **720**, the first section of data E2(A), and the second section of data E2(B) in encrypted form, are communicated from the encoder **10** to the decoder **20**, for example directly or via one or more proxy or relay servers of a data communication network, for example in a manner as illustrated in FIG. 6.

In the step **730**, the decoder **20** receives the encoded data E2(A), E2(B) and then optionally checks that the encoded data E2(A), E2(B) has been encoded by an authorized and validated transmitter **100**. In an event that the encoded data E2(A), E2(B) is acceptable, the decoder **20** proceeds to decrypt the encoded data E2(B) to generate one or more parameters required for decoding the encoded data E2(A) to regenerate a version of the data D1. Optionally, transcoding is employed in the decoder **20** when the data D1 has to be reformatted in relation to rendering facilities available in association with the decoder **20**, for example screen size, screen aspect ratio, screen resolution, screen rotation and such like.

In the step **740**, the decoder **20** renders the regenerated data D1, transcoded when required, to a user of the recipient **200** incorporating the decoder **20**.

Optionally, the encoder **10** and the decoder **20** are spatially collocated within one device, for example a smart phone, a video camera, a personal computer, a medical apparatus, a seismic apparatus, a satellite, a drone, a surveillance system, a video conferencing system and the encoded data E2(A), E2(B) is stored within the device and/or spatially externally thereto.

Techniques employed in embodiments of the present disclosure, as described in the foregoing, are optionally employed for military and medical purposes, in cases where very secure and reliable encryption is desired, but an unprotected telecommunications connection needs to be used between one or more recipients. The embodiments of the present disclosure provide a way to use known, but well tried-and-tested,

technology in a novel manner, which makes it possible for a given media content producer to decide who is allowed to see and/or hear the media content, thus offering a safe option to distribute and render media content both online and offline, regardless of a given transfer channel that is used

Modifications to embodiments of the invention described in the foregoing are possible without departing from the scope of the invention as defined by the accompanying claims. Expressions such as “including”, “comprising”, “incorporating”, “consisting of”, “have”, “is” used to describe and claim the present invention are intended to be construed in a non-exclusive manner, namely allowing for items, components or elements not explicitly described also to be present. Reference to the singular is also to be construed to relate to the plural. Numerals included within parentheses in the accompanying claims are intended to assist understanding of the claims and should not be construed in any way to limit subject matter claimed by these claims.

References:

[1] RSA (cryptosystem) - Wikipedia, the free encyclopedia (accessed November 27, 2014). URL: http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29

[2] "*Pretty Good Privacy*", PGP - Wikipedia, the free encyclopedia (accessed November 27, 2014). URL: http://en.wikipedia.org/wiki/Pretty_Good_Privacy

CLAIMS

1. A secure media player system for communicating media content information (D1) from an encoder (10, 100) to at least one decoder (20, 200), wherein the encoder (10, 100) is operable:

(a) to process and encode the media content information (D1) into one or more first sections of data (E2(A)) and one or more second sections of data (E2(B)), wherein the one or more second sections of data (E2(B)) include one or more parameters which enable the media content information (D1) to be regenerated from the one or more first sections of data (E2(A));

(b) to encrypt the one or more second sections of data (E2(B)) to generate corresponding one or more encrypted second sections of data (encrypt(E2(B))); and

(c) to communicate the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))) to the at least one decoder (20, 200) for the at least one decoder (20, 200) to process and render the media content information (D3) to one or more users,

characterized in that the secure media player system does not store or allow the at least one decoder (20, 200) to store the one or more encrypted second sections of data (encrypt(E2(B))) in an unencrypted form into a memory from which the one or more second sections of data (E2(B)) can later be downloaded in an unencrypted manner, wherein the secure media player system stores at the at least one decoder (20, 200) the one or more encrypted second sections of data (*encrypt*(E2(B))) in an encrypted form.

2. A secure media player system as claimed in claim 1, characterized in that the one or more encrypted second sections of data (*encrypt(*E2(B))) are encrypted using at least one encryption key that identifies the encoder (20, 200) when the at least one decoder (20, 200) processes the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))).

3. A secure media player system as claimed in claim 1, characterized in that the at least one decoder (20, 200) is provided with a complementary key to that used by

the encoder (10, 100) when generating one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))), wherein the complementary key is used by the decoder (20, 200) to process and render the media content information (D3) to the one or more users.

4. A secure media player system as claimed in claim 2 or 3, characterized in that the one or more keys are provided from at least one of: a validating authority, a certifying authority, a verification authority.

5. A secure media player system as claimed in claim 1, characterized in that the system is operable to customize uniquely the one or more encrypted second sections of data (*encrypt(*E2(B))) for each corresponding decoder (20, 200).

6. A secure media player system as claimed in claim 1, characterized in that at least the one or more first sections of encoded data (E2(A)) are communicated via at least one relay and/or proxy server which is operable to service a plurality of decoders (20, 200) with the encoded data (E2(A)).

7. A method of communicating media content information (D1) from an encoder (10, 100) to at least one decoder (20, 200) within a secure media player system, wherein the method includes:

(a) processing and encoding the media content information (D1) into one or more first sections of data (E2(A)) and one or more second sections of data (E2(B)), wherein the one or more second sections of data (E2(B)) include one or more parameters which enable the media content information (D1) to be regenerated from the one or more first sections of data (E2(A));

(b) encrypting the one or more second sections of data (E2(B)) to generate corresponding one or more encrypted second sections of data (encrypt(E2(B)); and

(c) communicating the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))) to the at least one decoder (20, 200) for the at least one decoder (20, 200) to process and render the media content information (D3) to one or more users,

characterized in that the secure media player system does not store or allow the at least one decoder (20, 200) to store the one or more encrypted second sections of data (*encrypt*(E2(B))) in an unencrypted form into a memory from which the one or more second sections of data (E2(B)) can later be downloaded in an unencrypted manner, wherein the secure media player system stores at the at least one decoder (20, 200) the one or more encrypted second sections of data (*encrypt*(E2(B))) in an encrypted form.

8. A method as claimed in claim 7, characterized in that the one or more encrypted second sections of data (*encrypt(*E2(B))) are encrypted using at least one encryption key that identifies the encoder (20, 200) when the at least one decoder (20, 200) processes the one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))).

9. A method as claimed in claim 7, characterized in that the at least one decoder (20, 200) is provided with a complementary key to that used by the encoder (10, 100) when generating one or more first sections of data (E2(A)) and the one or more encrypted second sections of data (*encrypt*(E2(B))), wherein the complementary key is used by the decoder (20, 200) to process and render the media content information (D3) to the one or more users.

10. A method as claimed in claim 8 or 9, characterized in that the one or more keys are provided from at least one of: a validating authority, a certifying authority, a verification authority.

11. A method as claimed in claim 7, characterized in that the method includes customizing uniquely the one or more encrypted second sections of data (*encrypt(*E2(B))) for each corresponding decoder (20, 200).

12. A method as claimed in claim 7, characterized in that at least the one or more first sections of encoded data (E2(A)) are communicated via at least one relay and/or proxy server which is operable to service a plurality of decoders (20, 200) with the encoded data (E2(A)).

13. A computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute a method as claimed in any one of claims 7 to 12.