

【DESCRIPTION】**【Disclosure Title】**

SYSTEM AND METHOD FOR MANAGING WATERMARK OF VR CONTENT
BY MEANS OF BLOCKCHAIN

【Technical Field】

[0001] The present disclosure relates to a method for managing a distribution process of a virtual reality (VR) content using a blockchain network, and more specifically, to a method for monitoring whether the watermark inserted into a VR content is tampered using a blockchain to prevent the illegal VR content from being used, and a system for the same.

【Background Art】

[0002] The intellectual property copyrights are interfered by the unauthorized copying and editing of a digital content such as a VR content.

[0003] To solve such a problem, in recent years, a technology of managing the behaviors such as the copy and distribution of the digital content using a blockchain such that the copyright fees may be wholly distributed to the true copyright holders has begun to be researched.

[0004] However, if the watermark is inserted into the video content, this may cause a visually annoying problem, and if the watermark is inserted so as not to obscure the view, there is a limit in that the watermark may be forged and

tampered in the method for deleting the watermark, or identically copying the watermark.

[0005] Particularly, content creators such as youtubers or broadcasting jockeys (BJs) make the profits in proportion to the number of views in the video, and if the content is unauthorizedly copied and distributed, the economic loss occurs and if the content is maliciously edited and distributed, the content may be analyzed contrary to the intention, thereby hurting the image.

[Disclosure]

[Technical Problem]

[0006] The present disclosure is devised to solve the above problem, and an object of the present disclosure is to provide a system and method for managing a watermark of a VR content using a blockchain, which may efficiently insert the watermark of the VR content and manage the watermark through a blockchain network, thereby fundamentally preventing the forgery and falsification or the illegal copy.

[Technical Solution]

[0007] To achieve the object, a system for managing a watermark of a VR content using a blockchain according to an exemplary embodiment of the present disclosure may include: a node connected to a blockchain network to generate a block recording transaction on the blockchain network; a producer terminal for inserting address information, which is

generated using a unique address value assigned by the blockchain network and key frame information of a VR content, and a watermark for protecting the copyright of the VR content into the VR content, and controlling transaction corresponding to a production behavior of the VR content to be recorded in a block of the blockchain network, upon authoring the virtual reality (VR) content; and a user terminal provided with a viewer for controlling transaction corresponding to a playing behavior of the VR content to be recorded in the block of the blockchain network, restoring the address information using the watermark inserted into the VR content, and transmitting verification information including information about the restored value and the viewer to the blockchain network, upon playing the VR content.

[0008] The producer terminal may insert the watermark into a frame spaced apart from each key frame of the VR content constantly forward or backward and divide and insert the watermark into both channels of the corresponding frame.

[0009] The node may determine whether the VR content is forged and falsified by analyzing the verification information received from the viewer of the user terminal.

[0010] The node may determine that the VR content is forged and falsified, and a key frame not including the watermark exists and perform exception handling, if a unique address value does not exist in the verification information received

from the viewer of the user terminal while the VR content is being played.

[0011] The node may determine that the VR content is forged and falsified, and a different watermark exists within a single file and perform exception handling, if a unique address value included in the verification information received from the viewer of the user terminal is changed while the VR content is being played.

[0012] The node may determine that the VR content is forged and falsified and perform exception handling, if a watermark, which is not restorable, exists in the VR content by analyzing the verification information received from the viewer of the user terminal while the VR content is being played.

[0013] According to an exemplary embodiment of the present disclosure, a method for managing a watermark of a virtual reality (VR) content by a node connected to a blockchain network to generate a block recording transaction on the blockchain network may include: producing, which assigns a unique address value on the blockchain network to a newly generated VR content according to the request from a producer terminal, and records transaction corresponding to a production behavior of the VR content in a block of the blockchain network; and playing, which records transaction corresponding to a playing behavior of the VR content

according to the request from a viewer playing the VR content in the block of the blockchain network, and determines, by the viewer, whether the VR content is forged and falsified by receiving and analyzing verification information generated using a watermark inserted into the VR content while the VR content is being played.

【Advantageous Effects】

[0014] The present disclosure may manage all processes of the production and distribution of the VR content using the blockchain network.

[0015] Further, when the unauthorized person arbitrarily edits or modifies the distributed VR content, the inserted watermark is falsified, but the present disclosure may confirm the falsified fact through the verification information collected from the viewer and perform the predefined exception handling.

[0016] Further, the present disclosure may also simply confirm the VR content through the transactional book of the blockchain if the VR content is distributed without authorization, thereby protecting the digital authoring and fairly distributing the copyright fee to the true copyright holder.

[0017] Further, any viewers who play arbitrarily edited or modified VR content deliver the information through the blockchain network if the arbitrarily edited or modified VR

content is illegally copied, distributed, or streamed, such that the present disclosure may perfectly protect the VR content even if the actor, who copies or distributes the VR content without authorization, from disabling the DRM means.

【Description of Drawings】

[0018] FIG. 1 is a diagram for explaining a configuration of a network of a system for managing a watermark of a VR content using a blockchain according to an exemplary embodiment of the present disclosure.

[0019] FIG. 2 is a diagram for explaining a method for inserting the watermark into the VR content according to the exemplary embodiment of the present disclosure.

[0020] FIG. 3 is a flowchart for explaining a method for managing the watermark of the VR content using the blockchain according to the exemplary embodiment of the present disclosure.

【Best Mode】

[0021] The terms used in the present specification will be briefly described, and the present disclosure will be described in detail.

[0022] As the terms used in the present disclosure, general terms currently, commonly used as possible while considering the function in the present disclosure are selected, but these may be changed according to the intent or cases of those skilled in the art, the emergence of a new technology,

or the like. Further, there are also the terms arbitrarily selected by the applicant in a specific case, and in this case, the meaning thereof will be described in detail in the detailed description of the corresponding disclosure. Therefore, the terms used in the present disclosure should be defined based on the meaning of the terms and the contents throughout the present disclosure rather than the name of the term simply.

[0023] Throughout the specification, when any portion "includes" any component, this means as further including other components rather than excluding other components unless specially otherwise described. Further, the terms such as " ... means", " ... part", and " ... module" described in the specification mean the units of processing at least one function or operation, and this may be implemented by hardware or software or a combination of hardware and software.

[0024] Hereinafter, an exemplary embodiment of the present disclosure will be described in detail with reference to the accompanying drawings such that those skilled in the art to which the present disclosure pertains may easily carry out the present disclosure. However, the present disclosure may be implemented in various different forms and is not limited to the embodiments described herein. Further, to clearly describe the present disclosure in the drawings, a portion

not related to the description will be omitted, and a similar portion is denoted by a similar reference numeral throughout the specification.

[0025] A blockchain is also called a public transactional book as a distributed data storage technology of storing data in a block to connect the data in a chain form, and simultaneously copying and storing the data in many computers. This is why the blockchain may send the transactional history to all users who participate in the transaction without storing the transactional history in a centralized server, and allow all transactional participants to share the information on each transaction and compare the information, thereby preventing the data from being forged or falsified.

[0026] When there is the transaction between A and B, the corresponding transactional block is generated and the generated block is transmitted to all participants on the network, and as a result, the mutual verification for the information of the block is completed and the block is coupled to a chain. When the cryptocurrency remittance transaction between the A and the B occurs in the cryptocurrency blockchain, the transferring histories including the cryptocurrency addresses, transfer amounts, and the like of the transactional parties will be also recorded in the block.

[0027] FIG. 1 is a diagram for explaining a configuration of

a network of a system for managing the watermark of a VR content using a blockchain according to an exemplary embodiment of the present disclosure.

[0028] A blockchain network 100 collects individual servers who participate in the transaction to maintain and manage the network without storing or managing the transactional records in the centralized server. The individual server, that is, the participant is called a node. The node is connected to the blockchain network to generate a block recording the transaction on the blockchain network.

[0029] Since there is no central manager, the role of the node distributing the block is important, and a new block is generated only when a half or more of the participating nodes are agreed. The nodes store the blockchain in which the transactional history, that is, the transactions are recorded in the computer, and even when some nodes are hacked and the existing contents go wrong, the data may remain in multiple nodes, thereby continuously preserving the data.

[0030] Each node of the blockchain network 100 is a mining subject which serves to verify whether the corresponding transaction is forged and mine a block in which the transaction is recorded to add the mined block to the blockchain by operating hash values of the entire book from a Merkle tree, and receives a commission according to the transaction in return.

[0031] A producer terminal 110 having an authoring tool 111, which is a means capable of producing the VR content, and/or a user terminal 120 having a viewer 121, which is a means capable of playing the distributed VR content, may be operated as the node participating in the blockchain network 100. In this case, the producer terminal 110 and/or the user terminal 120 may directly approach the blockchain network 100 to execute a smart contract related to the management of the VR content according to the present disclosure.

[0032] However, to be operated as the node of the blockchain network, the synchronization should be performed by continuously downloading the block data, such that the producer terminal 110 and/or the user terminal 120 may connect the blockchain data having a very large capacity to the node serving as a kind of server without directly storing the blockchain data to use the smart contract related to the management of the VR content according to the present disclosure.

[0033] In this case, the producer terminal 110 and/or the user terminal 120 may approach the blockchain network 100 using a remote procedure call or a predetermined access service through a web browser. The smart contract generated by the user on the network is recorded in the block and the corresponding code is also copied to other nodes, thereby executing the smart contract in a virtual machine of each

node.

[0034] The node of the blockchain network 100 records each of production, copy, and playing behaviors of the VR content in the book with the blockchain transaction according to the smart contract, thereby performing the necessary procedure. Upon the initial authoring of the VR content, a unique address on the blockchain network is assigned, and when the viewer 121 plays the VR content, a type of the transaction corresponding to the playing behavior is recorded in the corresponding wallet address of the blockchain book. The viewer 121 reads the watermark while the VR content is being played to generate verification information and provides the generated verification information to the blockchain network.

[0035] The node of the blockchain network 100 may determine whether the watermark is falsified from the verification information actively provided by the viewer 121, that is, whether the VR content is illegally, arbitrarily edited, modified, or distributed without authorization according to the smart contract.

[0036] Upon authoring the VR content, the producer terminal 110 inserts address information generated using a unique address value, which is assigned by the blockchain network 100 and key frame information of the VR content and the watermark for protecting the copyright of the VR content into the VR content, and controls the transaction

corresponding to the production behavior of the VR content to be recorded in the block of the blockchain network 100.

[0037] The user terminal 120 has the viewer 121, and upon playing the VR content, the viewer 121 may control the transaction corresponding to the playing behavior of the VR content to be recorded in the block of the blockchain network 100, restore the address information inserted into the content using the watermark inserted into the VR content, and transmit the verification information including the information about the restored value and the viewer itself to the blockchain network 100. The node may analyze the verification information received from the viewer 121 of the user terminal 120 to determine whether the VR content is forged and falsified.

[0038] FIG. 2 Is a diagram for explaining a method for inserting the watermark into the VR content according to the exemplary embodiment of the present disclosure.

[0039] The authoring tool 111 inserts the watermark upon authoring the VR content, that is, upon the initial production. The VR content is composed of two channels (left/right or top/bottom) and the watermark may be divided and inserted into both channels of each key frame 210. A part 230 of the watermark is inserted into a first channel and a remainder 240 of the watermark is inserted into a second channel.

[0040] Preferably, the watermark may be divided and inserted into both channels of a frame 220 spaced apart from each key frame 210 constantly forward or backward, thereby preventing the image quality from being lowered and preventing the watermark from being viewed by the eyes. For example, the watermark is inserted in a method of being inserted into the second frame from each key frame. When being inserted into the frame rather than the key frame, the watermark passes by in only 1/30 seconds upon playing a screen and the watermark is not well visible upon playing because the watermark is not inserted into the key frame. There is also an advantage in that it is difficult to find the watermark even in the case of flipping through or editing the watermark in units of key frame.

[0041] FIG. 3 is a flowchart for explaining a method for managing the watermark of the VR content using the blockchain according to the exemplary embodiment of the present disclosure.

[0042] In a step S31, an address value on a blockchain network is uniquely assigned upon authoring the VR content, that is, upon the initial production. Address information generated using the assigned unique address value and key frame information, and a watermark for protecting the copyright will be inserted into the generated VR content. The address information may be inserted by operating the corresponding

address value and key frame information by a predetermined operation formula to be divided and inserted into both channels of the key frame.

[0043] In a step S32, the production transaction of the VR content is recorded in the blockchain network according to the request from the producer terminal 110 authoring the VR content. Therefore, information indicating that the VR content using the unique address value on the blockchain network as identification information begins to be generated and distributed may be shared with all nodes participating in the blockchain network.

[0044] In a step S33, upon playing the VR content by the viewer 121, the playing transaction of the VR content is recorded in the blockchain network according to the request from the viewer 121. Therefore, the information indicating that the VR content using the unique address value on the blockchain network as identification information has been played by the specific viewer 121 at a specific time may be shared with all nodes participating in the blockchain network.

[0045] In a step S34, it is determined whether the played VR content is forged and falsified by analyzing the verification information received from the viewer 121 while the VR content is being played. The verification information received from the viewer 121 may include the information about a value obtained by restoring the address information using the

watermark inserted into the VR content and the viewer.

[0046] The viewer 121 may combine the watermarks divided and inserted into both channels of the VR content to restore the watermark through a predetermined operation formula, thereby restoring the address information including a specific address value of the blockchain network. The viewer 121 may transmit a flag indicating whether the VR content is streamed or played after being copied in addition to the address information restored using the predetermined operation formula and the identification information for the viewer itself as described above as the verification information upon playing the VR content.

[0047] The playing transaction occurs once from the playing start of the VR content to the ending time point of the VR content and is stored in the corresponding address on the blockchain network, but the verification information transmitted by the viewer 121 is periodically received by the degree at which the key frame exists and every time, whether the VR content is forged and falsified may be examined.

[0048] In a step S35, if it is determined that the VR content is forged and falsified, a predefined exception handling is performed. A type of forgery and falsification of the VR content and the exception handling will be described in detail below.

[0049] If the unique address value does not exist in the verification information received from the viewer 121 while the VR content is being played, it is determined that the VR content is forged and falsified and there is the key frame not including the watermark in the middle thereof and the exception handling is performed. Which VR content is forged and falsified may be identified by the information immediately before or immediately after received from the corresponding viewer, and which viewer plays the content may be identified by the viewer information (e.g., an IP address or the like). For the exception handling, the thus obtained forgery and falsification related information may be recorded in the blockchain and shared and also notified a predetermined external apparatus.

[0050] If the unique address value included in the verification information received from the viewer 121 while the VR content is being played is changed, it is determined that the VR content is forged and falsified, and a different watermark is included within a single file and the exception handling is performed. If a different address value is suddenly intercepted while the verification information is received from the viewer 121, the VR content may be determined as the forged and falsified content when a streaming section is not newly established, and the VR content is not played by unloading the existing file and

loading the new file.

[0051] If the watermark, which may not be restored, exists in the VR content by analyzing the verification information received from the viewer 121 while the VR content is being played, it is determined that the VR content is forged and falsified, and the exception handling is performed. If the watermark corresponding to any key frame is copied and illegally edited, and then copied in each key frame of the processed VR content, the address information may not be restored upon playing, such that the VR content may be determined as the forged and falsified VR content.

[0052] Even in the case of the VR content in which the watermark is entirely deleted, the viewer 121 may notify the blockchain network of the fact indicating that the VR content is played according to the header information, and the node of the blockchain network may determine the VR content as the forged and falsified VR content and the exception handling may be performed.

[0053] As described above, the production and distribution of the VR content may be managed using the blockchain network. When the unauthorized person arbitrarily edits or modifies the distributed VR content, the inserted watermark is falsified, and the falsification fact may be confirmed by the verification information received from the viewer 121, thereby performing the exception handling such as notifying

the producer or the copyright holder of such a fact, or recording the falsification fact on the blockchain network.

[0054] The method according to the exemplary embodiment of the present disclosure may be implemented in the form of a program instruction which may be performed by various computer means and recorded in computer readable media. The computer readable media may include program instructions, data files, data structures, and the like alone or in combination thereof. The program instructions recorded in the media may be ones specially designed and configured for the present disclosure or also ones known to and usable by those skilled in the computer software. As an example, the computer readable media includes magnetic media such as a hard disk, a floppy disk, and a magnetic tape, optical media such as a CD-ROM or a DVD, magnetic-optical media such as a floptical disk, and a hardware device specially configured to store and perform the program instructions, such as a ROM, a RAM, or a flash memory. As an example, the program instructions include a high-level language code executable by the computer using an interpreter or the like as well as a machine language code made by a complier.

[0055] As described above, although the exemplary embodiment of the present disclosure has been described in detail, the scope of the present disclosure is not limited thereto and various modified and improved forms by those skilled in the

art using the basic concept of the present disclosure defined by the appended claims also belong to the scope of the present disclosure.

【CLAIMS】

【Claim 1】

A system for managing a watermark of a VR content using a blockchain comprising:

a node connected to a blockchain network to generate a block recording transaction on the blockchain network;

a producer terminal for inserting address information, which is generated using a unique address value assigned by the blockchain network and key frame information of a VR content, and a watermark for protecting the copyright of the VR content into the VR content, and controlling transaction corresponding to a production behavior of the VR content to be recorded in a block of the blockchain network, upon authoring the virtual reality (VR) content; and

a user terminal provided with a viewer for controlling transaction corresponding to a playing behavior of the VR content to be recorded in the block of the blockchain network, restoring the address information using the watermark inserted into the VR content, and transmitting verification information comprising information about the restored value and the viewer to the blockchain network, upon playing the VR content,

wherein the VR content is authored in two channels by producer terminal,

wherein the watermark is inserted into a frame spaced

apart from each key frame of the VR content constantly forward or backward, and the watermark is divided and inserted into both channels of the frame,

wherein the watermark, divided and inserted into both channels, is combined and restored through a predetermined operation formula by the user terminal while the VR content is being played,

wherein it is determined whether the verification information comprising the restored watermark is forged and falsified by the node.

【Claim 2】

The system for managing the watermark of the VR content using the blockchain of claim 1,

wherein the node determines that the VR content is forged and falsified, and a key frame not comprising the watermark exists and performs exception handling, if a unique address value does not exist in the verification information received from the viewer of the user terminal while the VR content is being played.

【Claim 3】

The system for managing the watermark of the VR content using the blockchain of claim 1,

wherein the node determines that the VR content is forged and falsified, and a different watermark exists within a single file and performs exception handling, if a unique

address value comprised in the verification information received from the viewer of the user terminal is changed while the VR content is being played.

【Claim 4】

The system for managing the watermark of the VR content using the blockchain of claim 1,

wherein the node determines that the VR content is forged and falsified and performs exception handling, if a watermark, which is not restorable, exists in the VR content by analyzing the verification information received from the viewer of the user terminal while the VR content is being played.

【Claim 5】

A method for managing a watermark of a virtual reality (VR) content by a node connected to a blockchain network to generate a block recording transaction on the blockchain network, the method comprising:

producing, which assigns a unique address value on the blockchain network to a newly generated VR content according to the request from a producer terminal, and records transaction corresponding to a production behavior of the VR content in a block of the blockchain network; and

playing, which records transaction corresponding to a playing behavior of the VR content according to the request from a viewer playing the VR content in the block of the

blockchain network, and determines, by the viewer, whether the VR content is forged and falsified by receiving and analyzing verification information generated using a watermark inserted into the VR content while the VR content is being played,

wherein the VR content is authored in two channels by producer terminal,

wherein the watermark is inserted into a frame spaced apart from each key frame of the VR content constantly forward or backward, and the watermark is divided and inserted into both channels of the frame,

wherein the watermark, divided and inserted into both channels, is combined and restored through a predetermined operation formula by the user terminal while the VR content is being played,

wherein it is determined whether the verification information comprising the restored watermark is forged and falsified by the node.

【Claim 6】

The method for managing the watermark of the VR content using the blockchain of claim 5,

wherein address information generated using the unique address value assigned from the blockchain network and key frame information, and a watermark for protecting a copyright are inserted into the generated VR content, and

wherein the verification information received from the viewer of the user interface comprises: information about a value obtained by restoring the address information using the watermark inserted into the VR content and the viewer.

【Claim 7】

The method for managing the watermark of the VR content using the blockchain of claim 5,

wherein the playing comprises:

determining that the VR content is forged and falsified and a key frame not comprising the watermark exists and performing exception handling, if a unique address value does not exist in the verification information received from the viewer of the user terminal while the VR content is being played;

determining that the VR content is forged and falsified, and a different watermark exists within a single file and performing the exception handling, if the unique address value comprised in the verification information received from the viewer of the user terminal is changed while the VR content is being played; and

determining that the VR content is forged and falsified and performing the exception handling, if a watermark, which is not restorable, exists in the VR content by analyzing the verification information received from the viewer of the user terminal while the VR content is being played.