WHAT IS CLAIMED IS:

1. A method performed by a computing device for proving original, the method comprising:

generating an image by a photographing method based on a real subject discrimination algorithm, wherein the generating of the image comprises:

obtaining a screen division value for photographing the image;

dividing a photographing screen into a plurality of sections, based on the screen division value;

photographing a first image by focusing a first section among the plurality of sections;

photographing a second image by focusing a second section among the plurality of sections; and

storing the first image and the second image as the image;

obtaining proof data comprising the image and a challenge code for proving original of the image;

generating hash data by using the proof data;

generating signature data for the hash data;

transmitting the proof data, the hash data, and the signature data to a server; and

receiving an access path to an original verification result of the proof data from the server.

2. The method of claim 1, wherein the original verification result is generated according to a result of a verification, by the server, of the hash data, the signature data, and the challenge code.

3. The method of claim 1, wherein the transmitting comprises generating a transaction for recording the hash data in a blockchain network.

4. The method of claim 3, wherein the transmitting further comprises:

obtaining a transaction ID (identification) of the transaction; and

transmitting the transaction ID to the server.

5. The method of claim 3, wherein the server compares the transmitted hash data with hash data recorded in the blockchain network to verify the hash data.

6. The method of claim 1, further comprising:

providing the received access path to an external device.

7. The method of claim 6, wherein the external device includes at least one of an insurance company server, a trading brokerage site server, a law firm server, a media company server, and a public institution server, and the external device uses the access path to check the original verification result of the proof data.

8. A method performed by a computing device for proving original, the method comprising:

receiving proof data, hash data generated using the proof data, and signature data for the hash data from a user terminal, wherein the proof data includes an image which is photographed and a challenge code for proving original of the image, wherein the image comprises a first image and a second image, wherein the first image and the second image are images of photographing the same subject;

verifying the hash data, the signature data, and the challenge code, wherein the verifying comprises determining whether the image is an image of photographing a real subject, wherein the determining comprises:

obtaining a screen division value related to the image;

checking focused sections of the first image and the second image with reference to the screen division value; and

determining whether the image is an image of photographing a real subject based on a result of checking the focused sections;

generating an original verification result of the proof data based on a result of the verification of the hash data, the signature data, and the challenge code; and

transmitting an access path to the original verification result to the user terminal.

9. The method of claim 8, wherein the verifying further comprises:

verifying the hash data by comparing the hash data with hash data recorded in a blockchain network.

10. The method of claim 8, further comprising:

providing the original verification result of the proof data to an external device in response to a request of the external device through the access path,

wherein the external device includes at least one of an insurance company server, a trading brokerage site server, a law firm server, a media company server, and a public institution server.

11. A user terminal comprising:

a real subject photographing module for implementing a real subject discrimination algorithm and controlling a camera to generate an image according to the algorithm, wherein generating of the image comprises:

obtaining a screen division value for photographing the image;

dividing a photographing screen into a plurality of sections, based on the screen division value;

photographing a first image by focusing a first section among the plurality of sections;

photographing a second image by focusing a second section among the plurality of sections; and

storing the first image and the second image as the image;

a proof data generation module for generating proof data including the image and a challenge code for proving original of the image;

a hash extraction module for generating hash data by using the proof data;

a signature module for generating signature data for the hash data;

a communication module for transmitting the proof data, the hash data, and the signature data to a server; and

an access path management module for managing an access path to an original verification result of the proof data transmitted from the server.