

In order that the present invention may be fully understood and readily put into practical effect, an embodiment of the invention will now be described by way of non-limitative example, the description being with reference to the accompanying illustrative drawings, in which:

- 5 FIG. 1(a) is a schematic illustration of embedding data such as a message;
 FIG. 1(b) is a schematic illustration of extracting the embedded data of FIG. 1(a);
 FIG. 2 is a schematic illustration of block-by-block CRC embedding;
 FIG. 3 is a schematic illustration of two layers of watermarking;
 FIG. 4(a) is a Computed Tomography (CT) image;
- 10 FIG. 4(b) is the CT image of FIG. 4(a) after watermarking;
 FIG. 4(c) is an X-Ray Angiography (XA) image;
 FIG. 4(d) is the XA image of FIG. 4(c) after watermarking;
 FIG. 4(e) is an Ultrasound (US) image;
 FIG. 4(f) is the US image of FIG. 4(u) after watermarking;
- 15 FIG. 5(a) is a mammogram image;
 FIG. 5(b) is the mammogram image of FIG. 5(a) after tampering to add tumor-like
 features;
 FIG. 5(c) is the mammogram image of FIG. 5(b) displaying localization of the
 tampering;
- 20 ~~FIG. 5(c) is an X-Ray image;~~
 ~~FIG. 5(d) is the X-Ray image of FIG. 5(c) after tampering to add features that indicate~~
 ~~lung infection;~~
 ~~FIG. 5(e) is the X-Ray image of FIG. 5(d) displaying localization of the tampering;~~
 FIG. 5(d) is an X-Ray image;
- 25 FIG. 5(e) is the X-Ray image of FIG. 5(d) after tampering to add features that indicate
 lung infection;
 FIG. 5(f) is the X-Ray image of FIG. 5(e) displaying localization of the tampering;
 FIG. 6(a) is an XA image with 1 pixel of tampering;
 FIG. 6(b) is the XA image of FIG. 6(a) displaying localization of the tampering;
- 30 FIG. 6(c) is an XA image with an 8x8 pixel block of tampering;
 FIG. 6(d) is the XA image of FIG. 6(c) displaying localization of the tampering;
 FIG. 6(e) is an XA image with multiple 8x8 pixel blocks of tampering;

CLAIMS

1. A method of preparing a digital medical image for secure transmission, the method comprising:

embedding metadata into the digital medical image using a reversible watermarking process;

generating a code for tamper detection and localization from the digital medical image using a computational function; and

embedding the code for tamper detection and localization into the digital medical image using the reversible watermarking process;

wherein embedding the metadata using the reversible watermark process comprises dividing the digital medical image into non-overlapping pixel blocks, generating a random location signal designating one pixel of each non-overlapping pixel block as an estimator pixel, and embedding the metadata into one or more of the non-overlapping blocks as required.

2. A method of reviewing a digital medical image prepared by the method of claim 1, the method of reviewing comprising:

retrieving the code for tamper detection and localization from the digital medical image;

reversing the watermarking processes to obtain a restored image;

generating a code from the restored image using the computational function; and

comparing the retrieved code for tamper detection and localization with the code generated from the restored image to detect and locate tampering.

3. The method of claim 2, wherein generating the code from the restored image comprises dividing the restored image into non-overlapping pixel blocks and computing a cyclic redundancy code for each non-overlapping pixel block of the restored image~~A method of securely transmitting a digital medical image, the method comprising:~~

~~preparing the digital medical image using the method of claim 1;~~

~~transmitting the prepared digital medical image; and~~

~~reviewing the prepared digital medical image using the method of claim 2.~~

4. The method of ~~any one of the preceding claims 1~~, further comprising encrypting the random location signal using public key cryptography.
5. The method of claim 4, further comprising embedding a digital envelope into the digital medical image after embedding the metadata, the digital envelope comprising a concatenation of a bit stream of the encrypted random location signal, a cyclic redundancy code computed for the random location signal and a hash of the digital medical image.
6. The method of ~~any one of the preceding claims 1~~, wherein generating the code for tamper detection and localization from the digital medical image comprises dividing the digital medical image into non-overlapping pixel blocks and computing a cyclic redundancy code for each non-overlapping pixel block.
7. The method of claim 6, wherein embedding the code for tamper detection and localization using the reversible watermark process comprises embedding each cyclic redundancy code into the non-overlapping pixel block for which the cyclic redundancy code was computed.
8. A digital medical image prepared for secure transmission using the method of claim 1 or any one of claims 4 to 7~~The method of claim 2 and any one of claims 3 to 7 when dependent on claim 2, wherein generating the code from the restored image comprises dividing the restored image into non-overlapping pixel blocks and computing a cyclic redundancy code for each non-overlapping pixel block of the restored image.~~
9. ~~A digital medical image prepared for secure transmission using the method of claim 1 or any one of claims 4 to 7 when dependent on claim 1.~~A method of securely transmitting a digital medical image, the method comprising:
preparing the digital medical image using a method of:

embedding metadata into the digital medical image using a reversible watermarking process;

generating a code for tamper detection and localization from the digital medical image using a computational function; and

5 embedding the code for tamper detection and localization into the digital medical image using the reversible watermarking process,

10 wherein embedding the metadata using the reversible watermark process comprises dividing the digital medical image into non-overlapping pixel blocks, generating a random location signal designating one pixel of each non-overlapping pixel block as an estimator pixel, and embedding the metadata into one or more of the non-overlapping blocks as required;

transmitting the prepared digital medical image; and

reviewing the prepared digital medical image using a method of:

15 retrieving the code for tamper detection and localization from the digital medical image;

reversing the watermarking processes to obtain a restored image;

generating a code from the restored image using the computational function; and

20 comparing the retrieved code for tamper detection and localization with the code generated from the restored image to detect and locate tampering.