ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

A Survey on Watermarking and Reversible Medical Image Watermarking Techniques

Deepa S [1], Anitha Sandeep [2]

P.G. Student, Department of Computer Engineering, Mar Baselios College of Engineering and Technology, Nalanchira, Trivandrum, India [1]

Associate Professor, Department of Computer Engineering, BVM Mar Baselios College of Engineering and Technology, Nalanchira, Trivandrum, India [2]

ABSTRACT: Image authentication has drawn a good attention in both storage as well as communication, with the advancement of technology on the internet. Enforcement of protection of medical content that is being transmitted through the internet also has become a major issue of computer security. Since medical contents are more widely distributed, it is necessary to develop security mechanism to guarantee their confidentiality, authenticity and integrity. Lossless watermarking or reversible watermarking has been used, to provide security to the image as well as to any contents like Electronic Health Record(EHR). It overcomes the drawbacks of many ancient techniques that are already been used. In this paper, Region of Interest (ROI) and Least Significant Bit (LSB) based fragile watermarking techniques for tamper detection and recovery of medical images has been discussed.

KEYWORDS: Reversible Watermarking, Integrity, Confidentiality, Authentication, Medical Image Compression, ROI, LSB, EHR, RLE, tamper detection, DICOM, tamper recovery.

I. INTRODUCTION

Now a days transmission of medical images among hospitals over internet is a common practice. It can be done for many reasons which include teleconferences, tele-diagnosis, tele-consultation services and so on. Ensuring the security of exchanged medical data has become a major threat. The medical image security can be based on certain factors like (a) Authentication (b) Integrity (c) Confidentiality [7]

Authentication: It assures that the entity that is communicating is exactly the same person or organization that it claims to be. It can be used as a proof to ensure that the information is that of the right patient.

Integrity: It assures that the data obtained at the other end are same as what has been sent by the authorized sender (i.e., no insertion, modification, replay or deletion has occurred).

Confidentiality: The data can be protected from unlawful disclosure, ie., only the permitted user can have the right to use the information.

To offer security to the image as well as to any contents like Electronic Health Record (EHR) that is embedded into the image, techniques like encryption, digital watermarking, digital signature algorithms and digital fingerprint have been used. Copyright ownership can be identified using digital watermarking technique. Watermarking embeds or hides information into a cover image. A lot of watermarking algorithms exist, but most of them are lossy i.e. host image becomes permanently distorted due to the embedding process. It also causes a reduction in the peak signal to noise ratio (PSNR) value. A few applications like medical imaging, military etc, permanent reliability loss of the signal cannot be tolerated [6].

According to working domain, watermarking can be broadly divided as (a) Spatial domain (b) Frequency domain.

(a) Spatial Domain: The image pixel values are tailored directly in accordance to the watermark that need to be embedded. It is comparatively easy and also only less computation is needed. But the disadvantage is that it has got least security against any alterations. Most common spatial domain watermarking techniques include LSB, block based and SSM modulation techniques. Using LSB based, the most significant bit of some image is hidden into the LSB of

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

each selected pixel of the host image in accordance to some key value. Both host image and the watermark image which is binary is divided into blocks in case of block based technique. Then LSBs of each image block is set to zero and then a hash function like MD5 is applied to the image block. Then xor operation is performed against watermark image block and the hash function output and result is inserted into the least significant bit of the image block thus forming the watermarked image block. Reverse steps are performed for the extraction procedure. Energy that has been generated at distinct frequencies are purposely distributed in frequency or time domains and it is called spread spectrum technique. The most commonly used and preferred data hiding technique is LSB method. It is easier to implement, and can offer a better hiding or payload capacity. For medical image watermarking, spatial domain can be more suitable. It supports schemes like

(a) Substitutive Insertion (LSB Method) (b) Additive insertion.

(b) Frequency Domain: In the perceptually most significant components of frequency, a sequence is embedded. Watermark embedding is performed in DCT, DFT and DWT domain coefficients. The HVS is less sensitive to coefficients of high-frequency and more sensitive to coefficients of low frequency. Modifications to low frequency coefficients result in severe alteration to the original image, whereas high frequency coefficients are less significant. Therefore, techniques like compression, focuses in removing coefficients of high frequencies aggressively. Most algorithms embeds watermarks in the frequencies of midrange for obtaining a balance between robustness and imperceptibility. According to type of document, watermarking can be broadly divided as (a) Audio (b) Image (c) Video (d) Text

According to human perception, watermarking can be broadly divided as (a) Invisible (b) Visible. The visible watermarks can be implemented in areas like documents, images, multimedia files etc. Invisible watermark cannot be seen on the image directly, and so its presence need to be found out using some appropriate extraction techniques. Invisible watermark can be either robust or fragile. Fragile watermarks break down easily. In case of fragile watermark, it gets destroyed when watermarked content is modified or tampered with. Locality, transparency and security are a few major problems that need to be taken care of, when a fragile watermark is designed. Fragile watermarks are used to locate the tampered areas when the image has been tampered. Fragile watermarking is used for image authentication and tamper detection. Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. Attractive features of a robust watermark comprises of perceptual transparency, higher payload, resistance to geometric attacks, robustness against collusion attacks, computational simplicity, resistance to common signal processing operations like digital to analog conversion, compression, additive random noise etc.

Digital message authenticity can be proved using a mathematical scheme called digital signature. If a digital signature is valid, then the recipient can trust that the message has been generated by the expected sender and it has not undergone any alteration during transmission. Financial transactions or other cases which require great protection from tampering or forgery uses digital signature. The drawback of digital signature is that, using this technique only tamper detection is possible but not tamper localization.

To overcome the disadvantages of the methods like dig-ital fingerprint, encryption and digital signature algorithms, reversible or lossless watermarking has been proposed [9]. Conventional watermarking can help in retrieving the watermark but not the original cover image. But in case of reversible watermarking, the watermark is embedded into the host image and original image can be safely retrieved from the image that is suspected to be tampered. The watermark thus retrieved is compared with the original one so that the ownership can be well determined. The medical image should still conform to the digital imaging and communication in medicine(DICOM) image format even after watermarking has taken place.

Addressing of Integrity can be done at two levels [5], (a) strict integrity control in which one has to guarantee that the whole image is preserved as entire bit planes or (b) content-based control in which pixels are allowed to vary while the visual content meaning remains preserved. Cryptographic hash function can be used for achieving strict integrity.

Hash functions takes in some input of variable length m and produces output H(m) of a particular fixed length according to the hash algorithm used. A hash code is purely based only on the input message and not on any key value. Output obtained can be called as a message digest.

A medical image is first diagnosed and then only stored into any database, and hence the most important potion of that medical image can already be known. All medical images has got such a ROI (region of interest). It is the most important region of that medical image for having proper diagnosis. So, lossless recovery of the region of interest

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

portion of the medical image is mandatory at the receiver end.
Region of Non Interest (RONI) varies for different modalities. The most interesting feature of images like Ultrasound and all other medical images is that the LSB for all pixels in the RONI are generally zeroes [8].

A. Applications of watermarking

o Ownership declaration - A watermark signal can be generated using a secret private key, and can be embedded into the original document and then the document can be made publically available. So later any case of ownership issues can be easily resolved.

o Fraud and Tamper Detection - Tamper detection can be resolved by embedding fragile watermarks. The distortion, degradation or removal of fragile watermark indicates the presence of tamper and that the digital content cannot be trusted. In case of applications that deals with highly sensitive data like satellite imagery , military or medical imagery, tamper detection is of great importance. It is also important to ensure that the contents were originated from a specific source and that it had not been manipulated, changed or falsified. This fraud detection can be performed with the help of watermark.

o Security of ID cards - Some authentication information can be included in the persons photo that appears on the ID. Such information includes person's name, passport number etc. ID card verification can be performed by extracting those de-tails. The security level of those applications can be enhanced with the use of watermark. If a forged ID card is produced to perform fraud, the failure in extracting the watermark will invalidate the ID card.

o Copyright Protection - Redistribution of the materials, that are copyrighted, through un-trustworthy networks can be prevented using watermarking.

o Content Archiving - For archiving of digital contents like video, audio or images, serial number can be used. It can be inserted using watermarking techniques.

o Meta-data Insertion - Data about a data is termed as metadata. Audio files may consist of the name of the singer, the site which provided the particular copy etc as the meta data. In case of medical images like X-rays, patient health record could also be included as the metadata.

o Digital Fingerprinting - There are certain applications where multimedia content like audio, video etc are electronically distributed over network. In such cases, the owner of those contents would like to prevent unlawful distribution and duplication. This can be achieved by embedding in each copy of the content, a specific fingerprint. The owner of the digital content can be identified using digital fingerprinting. Fingerprints are unique to the owner of the digital data. The source of copies can be easily found out by extracting the fingerprint, if after sometime, unlawful copies of the data are found. Watermark is preferred to be invisible. It must not be vulnerable to intentional forging attempts or like attempts to remove them from the host data.

B. Properties of watermarking

o Robustness: Watermark should be resistant against al-terations of image and this ability is called robustness. It should not be possible to remove the watermark, or at least visible degradation of the source image should be avoided. A watermark must survive image modifications and all geometric distortions such as translation, scaling, rotation etc must be overcome by the watermark.

o No perceptibility: Even if a few bits of the cover are changed for embedding an invisible watermark, human visual system will not be affected.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

o Non Detectable: Invisible watermark must be designed in such a way that, it should not be detectable by any others including attackers.

o Complexity: It is the time taken for the process of encoding and decoding an image.

o Tamper Resistance: All type of attacks, whether it be with the motive to modify or remove, the watermark must be able to resist them all.

o Economically implementable: It depends on factors like time, effort and cost.

o Unambiguous: This means, it should be possible to make out the owner once the watermark has been retrieved.

o Capacity or Data payload: The amount of information that can be embedded into the image.

o Quality: Quality should not be degraded due to embed-ding of watermark.

o Fidelity or Transparency: Watermarking should not affect the quality of the original source image or introduce visible distortions. Distortions reduces the commercial value of the image.

C. Attacks on watermarking

o Unintentional attacks: A few manipulations are done on images to prepare them for printing which may include rotation, resizing, compression, sharpening etc.

o Malicious (intentional): They include attacks like altering existing watermark, disabling and also embedding new water-mark.

o Active Attacks : Purposely done by a hacker by trying to remove hacker tries to eliminate the existing watermark or make it unnoticeable by applying certain transformations like translation, scaling, rotation, change aspect ratio etc.

o Passive Attacks : In this case no damage or removal of watermark is made. Instead, the hacker just make attempts to determine whether a watermark is present and to identify it.

o Collusion Attacks : Hacker will be using different copies of the same piece of media. Every copy will be embedded with a different watermark, in order to make a copy with any watermark present.

o Forgery Attacks : Attacker, instead of removing the existing watermark, make attempts to embed legitimate watermark of their own.

o Presentation Attacks : Here watermark detection fails. It is due to introduction of several geometric transformations like scaling, rotation, translation, change aspect ratio etc.

Medical image watermarking techniques for the detection of tamper and its recovery using ROI and LSB based fragile watermarking techniques is reviewed in section 2 of this paper. In section 3 the experimental results of the discussed methods are studied and section 4 discloses the conclusion and future enhancements that can be done.

II. RELATED WORK

At first, a paper on fragile watermarking scheme [1] based on LSB (Least Significant Bit) and ROI (Region of Interest) for detection of tamper and the recovery of medical images has been studied. For that, first the division of medical

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

image into ROI and RONI is performed. Then, the authentication information is inserted into ROI and recovery information into RONI. Run Length Encoding (RLE) technique is used to compress and store the authenticating information in order to enhance the capacity of embedding in the region of interest, before actually inserting into ROI. Any tamper that has occurred to ROI of medical image is recognized and recovered with no loss according to the experimental studies. The LSBs of the region of interest and the hash value of ROI is together used in generating the fragile watermark. Hash value of the ROI is calculated using the algorithm, SHA-256. For an input to SHA-256, it produces a hash value of 256 bits which will be unique, which makes SHA-256 a better choice for hashing. In order to trim down the fragile watermark size, any data compression technique can be used. Lossless data compression is necessary in case of medical images. The compressed data can be used to reconstruct the original data at the receiver side [4]. The LSB's of ROI (Bp and Bp+1) is used to insert the generated fragile watermark. To effect tamper recovery of ROI, it is divided into 4x4 sized blocks, whereas RONI is divided into 3x3 sized blocks. It is assumed that the number of blocks in ROI and that in RONI are equal so that a 1-1 mapping can be established between both the blocks. The average intensity of pixels in each block and the parity of the average intensity is used for the calculation of 9 bit recovery information of each of the ROI blocks. LSB's of the respective blocks in RONI are used for storing the 9 bit recovery information. The watermarked image thus formed can now be transmitted via network to the destination. At the destination side, the information regarding the ROI is extracted from the pixels at the border of the watermarked image. Now, with the help of this extracted information, the received image can be separated into ROI and RONI. LSBs of ROI are used for the extraction of the fragile watermark that is embedded at the sender side. Now replace the LSBs of ROI using those retrieved LSB. Again compute the latest hash value of ROI and it is used for comparing with the extracted hash value. This check helps to figure out if any tampering has occurred to the ROI. In case of tampering, the recovery information already embedded can be used for the safe recovery of the ROI region.

The need for embedding more details like EHR paved way to review another watermarking method. In this second method [2], watermarking is performed as a combination of encryption techniques and data compression which is lossless. Watermark bits are scattered along the region chosen for embedding and also binary location map is used for locating the tamper which is a relatively new concept. All these makes this method a novel one. The entire image(ROI and RONI) is used for watermark embedding. If watermarked image remain unmodified, then ROI of the image can be completely recovered using this method. This method embeds two different watermark into the host medical image. One of watermark is formed using the patient health record(EHR) which is encrypted, keywords for indexing, identification code for doctor, information regarding ROI etc. All these are used at the receiver side while extracting information. The other watermark is used for the purpose of localizing where tamper has occurred and BLM is used for that purpose. Embedding process involves, taking the hash value of the region of interest using hash algorithm SHA-256, watermarked bit dispersion is done using an equation, insertion of the two watermark bits i.e. one in the penultimate bit plane for embedding more details like EHR, doctor identification code and so on and one in the LSB plane which is used for tamper localization purpose of the ROI. Watermark in the penultimate bit plane is composed of concatenation of hexadecimal representation of Bp and Bp+1, patient information encrypted using AES, number of vertices, vertex points, DIC and Hash of ROI which are compressed using compression techniques like arithmetic coding, SI in its binary representation form etc. After embedding the first watermark, further modifications are made in host figure so as to make it ready for tamper localization. Then for each 3x3 block, hash computation and bit selection is performed and the BLM (Bit Location Map) obtained is embedded into the LSB plane. At the extraction side, extract watermark from Bp+1th plane(penultimate plane) and separate SI and the compressed details and decompress those to get all those parameters. From those parameters define ROI, and replace the Bp and Bp+1 plane of ROI using binary value included among the compressed parameters and compute hash of ROI. Extract all bits of Bp bit plane and modify Bp to zeroes to get the modified watermarked image. Now compute BLM and compare with the one already extracted and also the computed hash value and the pre included hash value from sender side. If they both are same authentication result will be true and the technique terminates by extracting necessary value like PI, else find the difference of the extracted and the pre included binary location map to check where tamper has occurred.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

III. DISCUSSIONS AND OPEN PROBLEM

The technique used in the first paper was tested for quality by using PSNR value and found that the value is quiet high which indicates the watermarked image quality is high. Both tamper at a single location and also at multiple locations were also included purposefully and checked and it was found that the technique was successful in detecting all tampers and also in recovering ROI accurately. But in this technique RONI is not reversible. The second method is also RONI irreversible but it was successful in embedding further more information to become an all-in-one solution tool [2] for addressing several issues in relation to the management of medical information. This method was also tested for different modalities, image formats, bit rates etc. It have superior tamper localization property [2] and the entire process consumes only less time and executes faster. Security is ensured in this using several layers of techniques and has got a higher embedding capacity. The setbacks can be said as, the watermark payload of this technique is dependent on size of ROI and since two bit planes are used for embedding process, a slight higher degradation occurs even though it is not perpetually significant. Testing the technique on color images and also formulating an idea to reduce the degradation could enhance the technique for more wider use.

IV. CONCLUSION

The first method [1] discussed results in watermarked medical images of high quality. It helps to identify the presence of any tampers that might have occurred in ROI of medical images containing watermark with full accuracy. Also, the ROI part of medial image can be recovered with no loss. But here, the RONI is not reversible. Hence RONI is of least significance with respect to medical images, this limitation doesn't affects the usage of this technique. The second method [2] addresses many problems in relation to the management of medical information. In that, a blind and fragile watermarking technique is applied to the images. It also offers improved security, better capacity to embed and so on. This scheme is said to be tested for medical images of a wide variety of medical images like MRI, CT, US etc. This technique can locate even if a single pixel has been tampered and can produce the 3x3 block which is related to the region which is tampered. This scheme is quite feasible and simple. Both of these techniques are only ROI reversible. But as the second method can also embed many more details like EHR, doctor identification code and so on, it has got an upper hand over the first method. The second method can be made better by providing enhancements using which color images can also be tested [2].

ACKNOWLEDGEMENT

I would like to thank my guide and other faculty members of Mar Baselios College of engineering and technology, who provided their helping hands in the successful completion of this survey.

REFERENCES

[1] Eswaraiah, R., and E. Sreenivasa Reddy. "A Fragile ROI-Based Medical Image Watermarking Technique with Tamper Detection and Recovery."Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on. IEEE, 2014.
[2] Das, Sudeb, and Malay Kumar Kundu. "Effective management of medical information through ROI-lossless fragile image watermarking technique."Computer methods and programs in biomedicine 111.3 : 662-675, 2013.
[3] Gupta, Vinita, and Mr Atul Barve. "A review on image watermarking and its techniques." International Journal of Advanced Research in Computer Science and Software Engineering 4.1: 92-97, 2014.
[4] Chandramouli, R., Nasir Memon, and Majid Rabbani. "Digital watermarking."Encyclopedia of Imaging Science and Technology (2002).
[5] Pan, Wei, et al. "Medical image integrity control combining digital signature and lossless watermarking." Data privacy management and autonomous spontaneous security. Springer Berlin Heidelberg : 153-162, 2010.
[6] Singh, Suraj Kumar, Nilanjan Poria, and P. Palanisamy. "Reversible watermarking with embedded digital signature." Computation of Power, Energy, Information and Communication (ICCPEIC), 2014 International Conference on. IEEE, 2014.
[7] Umamageswari, A., and G. R. Suresh. "Performance Analysis Of Secure Medical Image Communication With Digital Signature And Reversible Watermarking." ictact journal on image and video processing 4.01: 647-651, 2013.
[8] Zain, Jasni M., L. P. Baldwin, and M. Clarke. "Reversible watermarking for authentication of DICOM images." Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE. Vol. 2. IEEE, 2004.
[9] Umamageswari, A., M. Ferni Ukrit, and G. R. Suresh. "A survey on security in medical image communication." International Journal of Computer Applications 30.3 : 41-45, 2011.