International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.121-123
DOI: http://dx.doi.org/10.21172/1.101.19
e-ISSN:2278-621X

ROI BASED WATERMARKING TECHNIQUE FOR IMAGE AUTHENTICATION

Shreya Talaulikar[1], Prof. Sherica Menezes[2]

Abstract-In recent years, the distribution of digital media les over an open channel using information and communication technology is increasing rapidly. This digital les may contain sensitive information. So providing security, authentication and robustness against attacks are still challenging issue due to attempts of hacking and malicious attacks by intruder. Watermarking can be an effective solution. Digital image watermarking is hiding secret data inside other multimedia. This paper presents a blind digital image water-marking approach of providing better content authentication and robustness against attacks in medical images. Our approach combines line-column hash function and Digital Signature to enhance authentication which will help additionally in tamper detection. Watermark will be embedded using 3-level DWT and pseudo-random sequence with the session key to get more PSNR ratio.
Keywords: ROI, RONI, Content authentication, on-line hash function, 3-level DWT, Session key,SHA-256,Pseudo Random Sequence.

1. INTRODUCTION

In the medical field, medical images such as X-ray, MRIs, CT scans, and Ultra-sound are transferred from one hospital to another for second guidance for process of diagnosis of patient disease. Therefore, special safety is required for medical images, because the diagnosis is done on medical images, which leads to the proper treatment. Otherwise, an undesirable outcome may result due to loss of decisive information [1]. Cryptography is the commonly used technique to protect digital content but it cannot provide facility to the owner to monitor as to how thecontent is handled after decryption. This limitation of cryptography may lead to illegal copying and misuse of the private information. The cryptographic techniques protect content in transit but after decryption of content, it has no further protection. Digital watermarking provides solution to above mentioned problems. Watermarking that protects the content even after decryption. Watermarking techniques embed imperceptible watermarking information into the main content such that the watermark is neither removed during normal usage nor causes trouble to the users [2].

Based on the working domain, watermarking methods can be divided into two categories spatial and frequency/transform domain techniques. In the spatial do-main technique, information is directly embedded in the image pixels and hence these methods are not robust and less secure against usual image processing attacks. This method manipulates intensity pixel values such method is Least Significant Bits (LSB). This is not the case for frequency/transform domain methods [3] where information is embedded into frequency coefficients of the image [4].Many different transform techniques such as discrete cosine transform(DCT) [5], discrete Fourier transform (DFT), discrete wavelet transform (DWT) [6] have been used.

This paper is ordered as follows section II Related work that covers previous research work carried on image watermarking. Section III introduction of DWT transform. Section IV presents proposed idea for an embedding and extracting process for enhanced authenticity. Section V presents Conclusion.

2. RELATED WORK

Several techniques have been proposed based on medical images each focusing on particular features.

Alavi Kunhu et al. have presented this method [7]. Aim of this method was the copyright protection and authentication of medical images. One robust watermark and one fragile hash-key watermark was embedded into the region of non-interest (RONI) in the wavelet domain using the discrete wavelet transform and second fragile hash-key watermark was embedded into the image RONI in the spatial domain. Since spatial domain was used for embedding that is less robust against attacks.

Lendale Venkateswarlu et al. [8] presented a robust watermarking algorithm for medical images using ARNOLD DWT. The watermarks inserted were invisible watermarks. There are two processes involved in this, embedding and extracting process. The cover image was scrambled using Arnold transformation and 2-level DWT was applied. The watermarks are inserted into the largest coefficients in LH/HL/HH bands. Watermarked images are obtained by applying the Inverse Discrete Wavelet Transformation (IDWT) and inverse Arnold transformation. While extracting, reverse of embedding process is followed on cover image and water-marked image. Disadvantage was it requires original image during extraction which may not be available.

[1] Department of Computer Science and Engineering, Goa College of Engineering, Goa, India
[2] Department of Computer Science and Engineering, Goa College of Engineering, Goa, India

Abhilasha Singh et al presented a scheme [9] were electronic health record and mean intensity value of ROI were used. The mean intensity was used with the intention of tampering malicious attack of replacing ROI with another one.The data was inserted into the RONI region. This technique done the isolation of ROI and RONI and was highly sensitive to attacks. This had the drawback of being tested only for lung CT scan images and also for not handling recovery process.
Zain et al have presented a method [10] in which data was randomly embedded in RONI using equations and also by randomly generating key for hashing which could provide more security. This method lacked any additional information regarding the patient i.e Patient Health Record which could make this method a more attractive one.

3. METHODOLOGIES USED

3.1 DWT Transform

DWT transforms a digital image into four sub-bands which provide approximation, vertical, horizontal and diagonal details. Using the low-pass filter and high-pass filter image is decomposed as LL, LH, HL and HH sub-bands [11]. Figure 1 shows DWT decomposition of image.

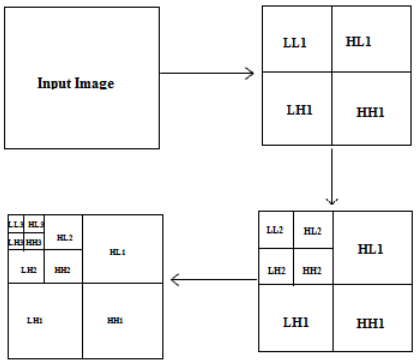

Figure 1: DWT decomposition of image

3.2 Digital Signature and line-column hash function

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing data creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature. A digital signature can be used with any kind of message whether it is encrypted or not, simply so the receiver can be sure of the sender's identity and that the message arrived intact [12, 13].
Here extracted ROI from the original image is taken and separate hashes are obtained for each column of an ROI. These hashes will then be digitally signed using an digital signature algorithm such as a private or public key system to increase the overall security and then hash data will be embedded in the RONI using LSB technique. Verifying procedure will consist of:
(1) Extracting ROI and calculating hash value of each column and digital signature algorithm will be used to sign this data.
(2) Extracting the embedded data and then comparing these two signatures to decide whether the image is authentic or not.

4. PROPOSED WORK

This technique will have three processes:

4.1 Separation of ROI

- First Convert input image to gray scale.
- Divide image into ROI and RONI part .It will return Xmin,Xmax, Ymin, Ymax pixel values of selected ROI region and image of selected ROI.
- Divide RONI into two areas called area1 and area2.

4.2 Embedding Process

The watermark is embedded in the region of non interest (RONIs) that have been selected in the previous step. For a hash to be embedded in a given RONI area1, the embedding is done as follows:

- First ROI is extracted and its hash of each column is calculate as mentioned above in section 3 in digital signature and line-column hash functions authentication using digital signatures on page 3.

For a watermark to be embedded in a given RONI area 2, the embedding is done as follows:

- An area 2 selected for embedding.
- A 3-level discrete wavelet transform (DWT) is calculated for area2. Watermarked image is taken and converted into 1D Vector.
- Pseudo random 2D sequence is generated by the session based key.
- HH3 sub band of the area2 is modified by using PN sequence and de-pending upon the content of the secret 1D image vector to be embedded.

The general equation used to embed the secret image is:

IS(x; y) = I(x; y) + k s(x; y)

In which I(x, y) representing the selected DWT sub band of the area2, IS(x, y)) is the modified area2 of image, K denotes the amplification factor that is usually used to adjust the invisibility of the secret image in corresponding sub band. S (x, y) is the pseudo random sequence.

- After embedding the watermark into area2 of RONI, Inverse DWT is applied to combine sub bands including modified sub band to generate the Watermarked image.
- Coordinates of ROI will be stored in border pixel.

4.3. Extracting Process

For a watermark to be extracted from RONIs area1, the extracting is done as follows:

- Watermark image will be input
- First ROI and RONI will be separated extracting the coordinates stored in border pixel of RONI of watermark image
- Calculate hash of each column of ROI and apply digital signature algorithm with public key of sender to obtain signed hash (s2)
- Extract signed hash (s1) in RONI of area1 and compare s1 and s2 to detect whether the image is authentic or not.
- Image content is said to be authentic if s1=s2 else not authentic.

For a watermark to be extracted from RONI area 2, the extracting process is done as follows:

- A 3-level discrete wavelet transform (DWT) is calculated for area2
- After applying 3-level DWT select the HH3 sub-band of watermarked image. Session key, sizes of the HH3 sub band and watermark image is sent to the receiver.
- With the help of same session based key which was used in the embedding procedure the pseudo random sequence (PN) is regenerated.
- The correlation between the selected watermarked sub-band and the generated pseudo random sequence is calculated.
- Each correlation value is compared with the mean correlation value. The extracted watermark bit is taken as a 0 if the calculated value isgreater than twice of the mean otherwise 1
- The recovery process then iterates through the entire PN sequence until all the bits of the watermark image have been recovered.
- After extraction process, Inverse discrete wavelet transform is applied to generate the original image.

5. CONCLUSION

There exist various medical image watermarking algorithms which provide the confidentiality of medical data, recovering original image without any distortion, data integrity, and authentication. Also the different segmentation algorithms are in place, which vary for the types of medical images such as MRI, CT scan, X-ray and Ultrasounds etc.

In proposed approach separation of ROI from the medical image will be done using mouse clicks where the ROI region is present which will be applicable for all types of medical images. Separated ROI can be stored with xmin,xmax, ymin, and ymax coordinate value. It will also check if image content is authentic or not and provide robustness against attacks.

6. REFERENCES

[1] Vandana S. Inamdar, Sonika C. Rathi," Medical Image Authentication through Watermarking Preserving ROI", International Journal, 2012. http://airccse.org/journal/hiij/papers/1112hiij04.pdf

[2] Ghanshyam Singh Anand Mohan Amit Kumar Singh, Basant Kumar. "Medical image watermarking techniques and applications", 2017. http://www.springer.com/in/book/9783319576985.

[3] Elizabeth Chang Vidyasagar M. Potdar, Song Han. "A survey of digital image watermarking techniques", 2005 http://ieeexplore.ieee.org/document/1560462/.

[4] Lalit Kumar Saini and Vishal Shrivastava. "A survey of digital watermarking techniques and its applications". International Journal of Computer Science Trends and Technology (IJCST), 2014.

[5] Jasdeep Singh, Blossom Kaur, Amandeep Kaur,"Steganographic approach for hiding image in DCT domain" International Journal of Advances in Engineering and Technology, 2011. https://pdfs. semanticscholar.org/70fb.

[6] Agya Mishra AkhilPratapShing. "Wavelet based watermarking on digital image". Indian Journal of computer Science and Engineering, 2011

[7] FatmaTaher, AlaviKunhu and Hussain Al-Ahmad. "A new multi watermarking algorithm for medical images using DWT and hash functions". IEEE, 2015

[8] B Eswara Reddy Lendale Venkateswarlu and N Vyaghreswara Rao. "Arnold - wavelet based robust watermarking technique for medical images", IEEE, 2016.

[9] Singh and Malay Kishore Dutta. "A blind and fragile watermarking scheme for tamper detection of medical images preserving ROI". In Medical Imaging, m-Health and Emerging Communication Systems, 2014.

[10] Jasni Mohamad Zain and Malcolm Clarke. "Reversible region of noninterest (RONI) watermarking for authentication of DICOM images".

[11] Pratibha Sharma and Shanti Swami. "Digital image watermarking using 3-level discrete Wavelet Transform". 2013.

[12] "Methodologies for watermarking techniques"

[13] Rita Noumeir, Adil Haouzia. "Methods for image authentication: a survey". 2007.