Crypto-Watermarking Algorithm For Medical Images Security

Sini Thankachan[1], Anju Rachel Oommen[2], Smita C Thomas[3]
[1, 2, 3] Dept of Computer Science and Engineering
[1, 2, 3] Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala

Abstract- *Advancements in information and communication technologies facilitated sharing of digital medical images in telemedicine applications. Widespread use of telemedicine applications demands a secure scheme to guarantee confidentiality and verify authenticity and integrity of exchanged medical data. This paper proposes an efficient crypto-watermarking algorithm to secure medical images transmitted for various tele-medicine applications. The proposed algorithm makes use of watermarking techniques combined with standard encryption techniques to provide confidentiality and authentication. Two watermarks are embedded in the image, histogram wrapping reversible data hiding algorithm. It enables verification of authenticity and integrity in both domains. Confidentiality is achieved using encryption of image. Partial encryption is used in the algorithm by selecting majority of pixels for embedding a watermark in a reversible manner. Reversible data hiding provides the flexibility of extraction of watermark and original image which contribute to the verification of integrity. The algorithm performs well in terms of different modalities of medical images.*

Keywords- Cryptography, Histogram Shifting, Shuffling, Watermarking, Wrapping.

I. INTRODUCTION

Medical images are being used in wide variety of tele-medicine applications like tele-surgery, tele-diagnosis, tele-conferencing, etc. The ease of copying, manipulation, exchange, and distribution of images across the vulnerable public networks have brought forth the importance of providing security to exchanged medical images. To provide safe transmission of medical images, there exists some security requirements that must be met. These requirements are confidentiality, authenticity, and integrity. Confidentiality states that only authorized users have access to the exchanged image, authenticity allows verification of the origin and owner of the exchanged image, and integrity ensures that the exchanged image has not been modified or tampered with. Security tools which are being used have many limits. Regarding the information system access, firewalls provide a certain level of isolation between the intra-net and Internet, but are easily bypassed by hackers. For storage and transmission, cryptography is probably a very efficient tool, but once the sensitive data is decrypted, the information is not protected anymore. Furthermore the file headers are in the plaintext format and can be usurped by a pirate. Watermarking is made to introduce identifiers which, by construction, are inseparable from the document they are attached to. They may be seen as ultimate ramparts against usurpation and fabrication. Encryption can be considered as a pre protection mechanism because, once decrypted or its digital signature deleted or lost, the information is no longer protected and it becomes hard to verify its integrity and its origin. Watermarking can be considered as a post protection mechanism as the image content is still available for interpretation while the remaining is protected. Thus, it is regarded as a complementary technique since it doesn't achieve confidentiality. This paper combines the advantages of encryption and watermarking together.

II. LITERATURE REVIEW

Large number of researches and studies are being conducted in the fields of security of images, especially in medical field. Different types of watermarking methods are being used to provide the security services required for telemedicine applications. These methods are divided into irreversible and reversible methods

A critical review of security practices currently used is provided in [1] and it introduces watermarking as a complementary element in the context of medical information security. It can be claimed that, in the medical domain, watermarking is an additional tool in the repertoire of security measures, specifically adapted to images, which can be used to thwart certain attacks.

The technique proposed in [2] uses Digital signature Embedding and extraction algorithm for medical images security. It has limitations like absence of scope of confidentiality mechanisms like encryption in the proposed method and authentication is ensured by digital signature embedding, but confidentiality is not ensured and proposed

method makes use of LSB shifting algorithm for embedding signature by which image can be distorted by opponent.

[3] gives a review on DES, AES and Blowfish for image encryption and decryption and it states that AES is the best image encryption algorithm security of images.

A reversible data hiding algorithm, which can retrieve the original image and the data without any distortionacted is given in [4]. This algorithm makes use of the zero or the minimum point of the histogram and modifies the pixel values to embed data. But the proposed algorithm is not a blind data hiding algorithm.

A technique to ensure authenticity and integrity of medical images is proposed in [5]. It has various limitations like it requires segmentation process to outline the boundary of body segment and in case of images without boundary; it may alter some vital pixel values. Also, it demands receiver's public key to generate Digital Envelope and this makes it difficult to integrate it in large scale imaging systems.

.

III. EXISTING SYSTEM

As medical images are highly sensitive to tampering, it is very important to restore the actual image from watermarked image and verify the integrity. Existing system makes use of histogram shifting for ensuring a reversible watermarking. The method has various advantages which overcomes the limitations of conventional Least Significant Bit insertion algorithm.

A. Data Embedding algorithm:

1. 1.Find a zero point in the histogram, e.g. 255, i.e., no pixel holds the gray value of 255 in the image. Then find the peak point, e.g. 154, i.e., a maximum number of pixels in the image has the gray value of 154.
2. Scan the whole image. Increment the gray value of pixels with gray value between 155 and 254 by "1". This is same as shifting the range of the histogram [155,254] to the right by one unit. Now, the gray value 155 empty.
3. 3 . Scan the whole image once again. Once a pixel with gray value of 154 is encountered, we check the data to be embedded. If the bit to be embedded is "0", the pixel value is kept as such. Otherwise, if it is "1"the pixel value is added by 1.

B. Data retrieval algorithm:

1. Scan the whole marked image. And check for the peak value. If the value is intact, e.g., 154, the "0" is retrieved. If the value is altered, e.g., 155, the "1" is retrieved. Retrieve the embedded data in this way.
2. Scan the whole image once again. Subtract the gray value of pixels between the peak point by 1. Thus, the original image can he recovered without any distortion.

This method has various advantages like low distortion in the watermarked image, fewer computational requirements and efficient data embedding capacity. The Histogram Shifting method is not blind since the side information, such as the minimum point or zero point and the peak point must be transmitted along with the watermarked image to enable the receiver side extract the hidden watermarks. Existing system overcomes the problem of non blindness of histogram shifting approach by embedding peak value and zero value in the image that is being the transmitted. This problem can be overcome by embedding the side information in the least significant bits of a selected group of pixels in the boundary regions of the image into which the data is to be hidden. However, limitation of existing system is that it modifies most of the pixel values which don't actually carry secret data.

IV. PROPOSED SYSTEM

The proposed algorithm uses a separable and reversible data hiding. It makes use of multiple data hiding techniques: one in spatial and one in encrypted domain. Interference is avoided using partial encryption and reversible data hiding. Initially, image is shuffled and divided to two parts. A larger and smaller part and separate watermarking is applied for both the parts. AES encryption is done for the larger part. Reverse process id done to extract the image during decoding.

A. The Encoding process

The data embedding procedure involves three main stages. In the first stage, the pixels of the cover image are randomly shuffled, and then divided unequally into two parts; a small part and a large part. In the second stage the two parts are watermarked with different watermarks. In the third stage, the large part is encrypted using the AES encryption standard, and is combined with the watermarked small part. The embedding procedure is described in details hereafter, and a block diagram illustrating the overall embedding operation is shown in Fig. 1

Step1: Shuffle the pixels of the input medical image using a random key.
Step2: Group 90% of the shuffled images into an array and rest 10% into another array. This small part provides integrity to the image after the large part is decrypted.
Step3: Embed the small watermark (SW) to the smaller part using the Histogram wrapping reversible hiding technique.
Step4: Embed the large watermark (LW) to the larger part using the same Histogram wrapping reversible hiding technique.
Step5: Encrypt the larger part using AES standard encryption algorithm
Step6: Join the two parts together and restore the pixels to obtain the crypto watermarked image,i.e. watermarked and encrypted image.

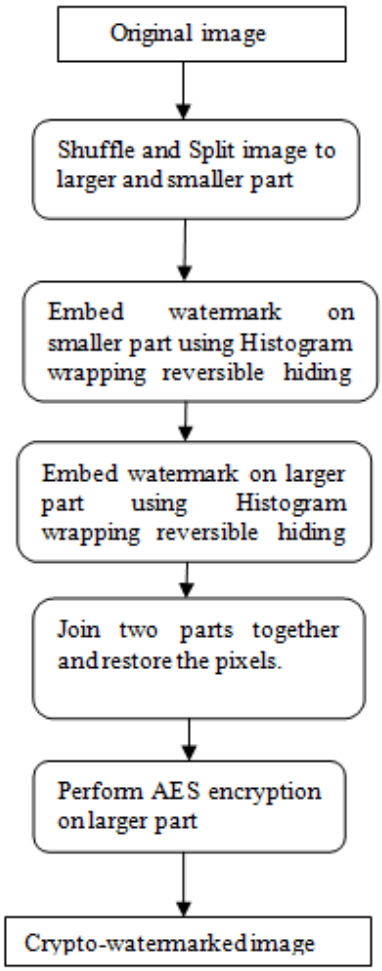

Fig 1: The Encoding Process

B. The Decoding Process

The decoding period is the direct reversal of the encoding procedure. Steps are explained below:

Step1: Shuffle the pixels of the input medical image using the same random key which is used in encryption.
Step2: Split the image into larger part and smaller parts.
Step3:Retreive water mark from the smaller part.
Step4: Decrypt the larger part using AES decryption.
Step5: Extract the watermark embedded in the larger part of image.
Step6: Join the two parts together and restore the pixels to obtain the original image.

4.1 WRAP AROUND HISTOGRAM SHIFTING

In almost every histogram shifting method, many pixels that don't hide the secret data are changed. However, if the modulo operation is used, the number of changing pixel is reduced. In modular arithmetic, numbers "wrap around" upon reaching a given fixed quantity. The peak point is distributed to close zero and the zero point is distributed to close $m-1$. Using character of wrap around, the histogram is directly shifted to the zero point from the peak point for the high quality. This method has a condition. Only if one or more zero point exists in histogram recovers the cover image. In Fig.3 shows the range of shifting on modulo 9. The peak point and zero point is 0 and 7. In the general histogram shifting, the range of shifting is 0 to 7 that is almost all pixel. However, in the wrap around histogram shifting, the range of shifting is 0, 7 and 8 that about 10,000 pixels are modified.

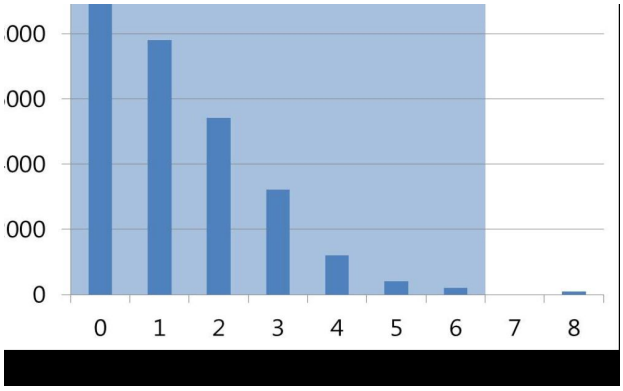

Fig 2: General Histogram Shifting

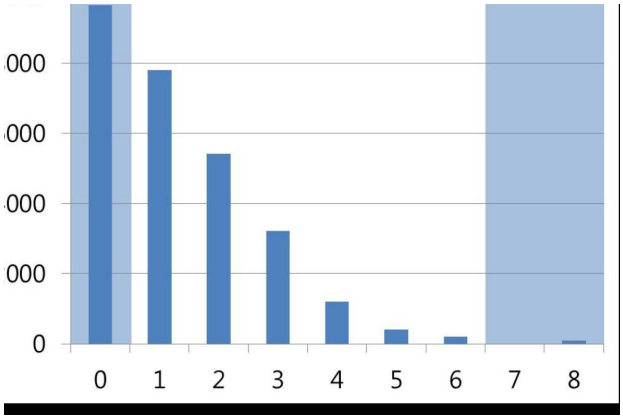

Fig 3: Wrap around Histogram Shifting

V. CONCLUSION

A separable joint crypto data hiding algorithm is used in this paper for medical images security. The algorithm jointly embeds two watermarks in two domains using encryption and watermarking to avoid any interference. The authenticity and integrity of medical images can be verified either in the spatial domain, i.e., after decrypting the image, or in the encrypted domain or in both domains. This avoids the overhead of decrypting the image each time to verify the integrity of image. Also, the proposed technique uses a reversible technique for watermarking, i.e, the original data can be retrieved removing the watermark.The algorithm can be applied to medical images since it offers an exact cover image reversibility without any errors in the extraction phase.

VI. ACKNOWLEGEMENT

We would like to thank, Almighty God at first, without his grace and blessings this work would not have been possible. We would also like to thank the faculty members of Mount Zion College of Engineering, for their great support towards this work.

REFERENCES

[1] Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R.,"Relevance of watermarking in medical imaging", in Proceedings of the IEEE EMBS Conf. on Info. Technology Applications in Biomedicine, Arlington, USA, (2000) 250-255Zhou, Z., Huang, H.

[2] Liu, B., "Digital signature embedding (DSE) for medical image integrity in a data grid off-site backup archive," in Proc SPIE 5748: (2005) 306-317.

[3] Aarti Devi, Ankush Sharma, Anamika Rangra,. "A Review on DES, AES and Blowfish for Image Encryption and Decryption ". International Journal of Computer Science and Information Technologies, Vol.6(3), 2015.

[4] Zhicheng Ni, Yun Q. Shi, Nirwan Ansari and Wei Su, Reversible Data Hiding", IEEE Transactions on Circuits and Systems for Video Technology,,Vol 16, Issue 3, 2006.

[5] X. Q. Zhou; H. K. Huang; S. L. Lou "Authenticity and integrity of digital mammography images" IEEE Transactions on Medical Imaging, Volume: 20, Issue: 8, 2001