ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

IMAGE WATERMARKING USING SECURE HASH ALGORITHM

G.Swathi
Dept. of Electrical and Electronics Engineering
Tiruchengode, India.
Swathiswathi1192@gmail.com
M.Senthil Kumar
Asst. professor, Dept. of Electrical and Electronics Engineering,
Tiruchengode, India.

Abstract:**The medical data is needed to be securely transferring information over the public network and manipulated effectively. The medical image watermarking method is used for enhancing security and authentication of medical data which is used for further diagnosis and references. So there is great need of elimination such illegal copyright of digital media. Digital watermarking is the powerful solution to this problem. The information is embedded in image which is used in some other applications as fingerprint; owner identification etc. The paper proposes SHA 256, AES (Advanced encryption standard) and arithmetic coding techniques. The ROI of medical image is irregularly shaped and it is an area which contains important information. The medical image and protection of information, and SHA 256 of the whole image is embedded in the least significant bits of the ROI (region of interest).SHA 256 of the recovered image will be compared with the extracted watermarking for authentication. Fragile watermarking scheme can detect tamper and recover the images. The watermarking technique being developed to confirm and simplifyfilesverification, safety and copyright protection, privacy protection, safety and management of digital media.**

Keyword: Watermarking, AES (Advanced Encryption Standard), ROI, RONI, SHA-256.

I. INTRODUCTION

Medical information is highly valued and critical due to its importance in clinical diagnosis, treatment, research, education and otheruses, both for private and government organizations. Due to the rapid and significant changes of information and communication technologies medical data distribution and organization systems have undergone aimportant change both in concepts and applications. Medical imaging plays a vital role in telesurgery, telediagnosis. Multimedia and cable technologies need different means of remote access and sharing of patient data. In medical data distribution and management systems, several security issues are occurred. The security issues are named as confidentiality, availability and reliability. In confidentiality issue refers the patient data is accessed by only authorized users. The availability issue guarantees the medical information has to be access. The reliability issue is based on integrity and authenticity. This provides a proof that the medical information has not been modified or hacked by the unauthorized users. In medical image watermarking, the image is divided into two regions:

ROI (region of interest)

- ROI area is depending on the availability of clinical finding and its features in the medical image.

RONI (region of non interest)

- RONI is the background or any area, is not a clinical finding.

Process of securing medical images through watermarking ROI can be applied on the remaining part of the image called as Region of Non Interest (RONI). The medical image and should not undergo any modification in Region of Interest. There can be several disjoint ROIs in a medical image and a number of ways exist to define the ROI in a medical image: manual, automatic. A polygonal ROI can be defined by the user (medical doctor, clinician, etc.) interactively. The reason of selecting polygonal ROI in a medical image is irregularly shaped.

II.METHODOLOGY

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

We have used some ordinary tools, like SHA-256, Advance Encryption Standard (AES) and compression in our proposed scheme. SHA-256 is used to calculate the hash of the ROI of the medical image. This hash is used in some other medical image. In our algorithm,AES cryptographic method is used to encrypt/decrypt the EHR/DICOM metadata part to completeenhanced security. To reduce the payload's size we lossless compressed the watermark using arithmetic coding.

2.1 HASH OF ROI

The ROI is the most important part of medical image. It contains the most valued information of the medical image and should not undergo any modification. There can be someseparate ROIs in a medical image and several ways exist to define the ROI in a medical image. In the standard DICOM file format if the ROI is present is embedded in a tag of the DICOM header. In the new method is used in the polygonal ROI can be defined by the user (medical doctor, clinician, etc.) interactively. Although, only I have concentrated on single ROI, the proposed method. After the selection of the ROI, the hash of the ROI is computed using the SHA-256 hash function,

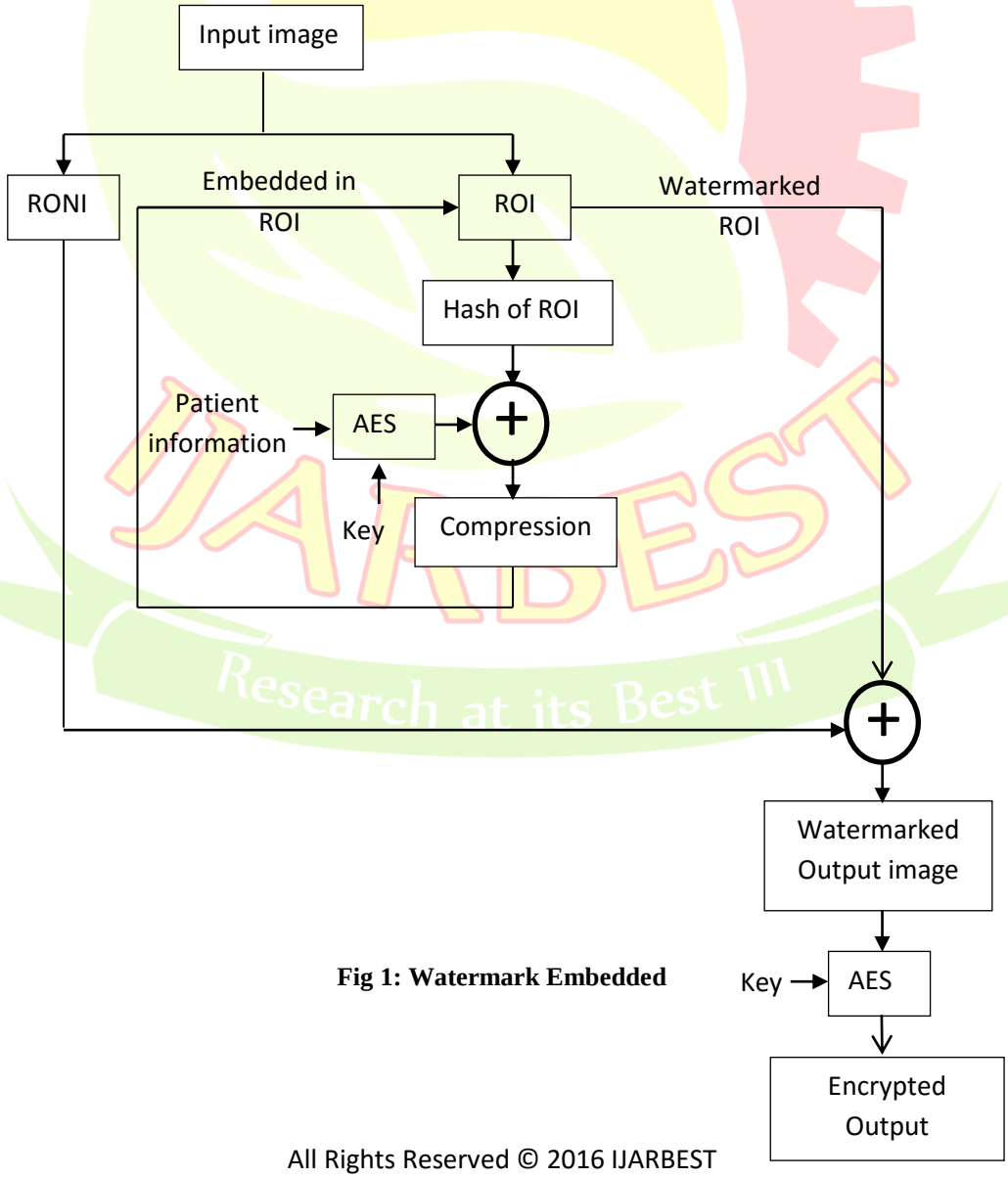


Fig 1: Watermark Embedded

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

which produces a 32 byte (256 bits) message digest.The SHA (Secure Hash Algorithm) is one of a digit of cryptographic hash functions. A cryptographic hash is like a monogram for a text or a data file. SHA-256 algorithm produces an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back. This types it suitable for keyword authentication, challenge hash authentication, anti-tamper, digital signatures.

2.2. WATERMARK EMBEDDED

The original MRI image ROI and RONI separated. The medical images can be transferredsecurely by embedding watermarks in ROI is allowing verification at the receiving end without affecting ROI. Subdivision is important rolein medical image to separating the ROI health image.

Steps:

1. Separate Original Image into ROI and RONI.
2. Compute the message digest HASH of ROI using SHA- 256.

Image, as binary strings respectively.

3. Change OI-Binary and ROI-Binary to their bit-stream and cell representations as and BP (Binary Pattern).
4. Embedded using LSB- Bits.
5. Create the binary string representation of BP as LSB.
6. Represent LSB to its equivalent binary bits form as Hex of OI.
7. Concatenate nv, v(x, y), IDX (Index of Bit stream), BP, LSB and OI-LSB Bits to get WMCONCA

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Assuming, Original Image and ROI represents the bit-planes of the ROI, numbered OI and OIROI + 1 respectively. Represent the pixels of Original

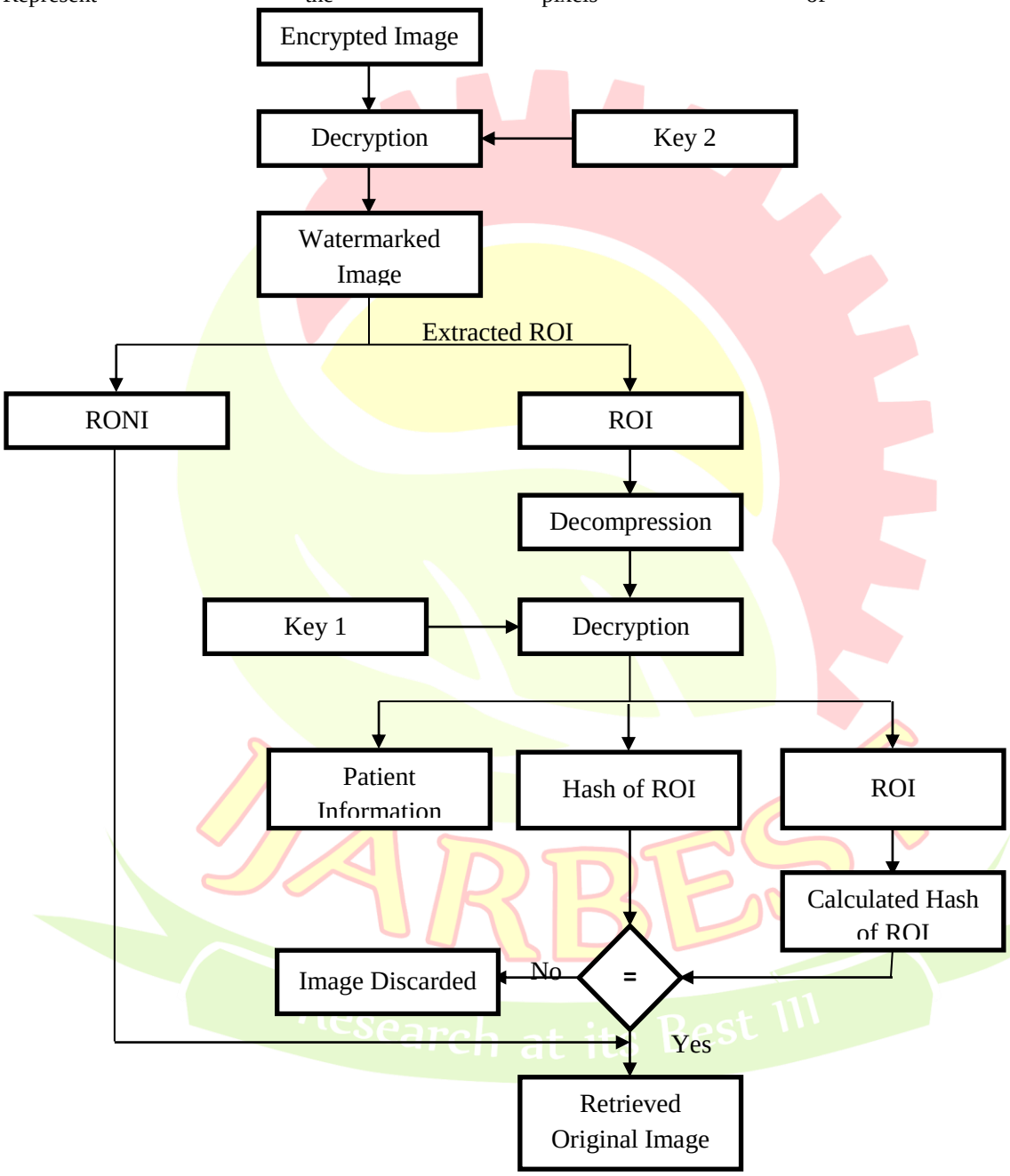


Fig 2: watermark extraction

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

8. Compress WMCONCAT lossless to WMCOM using arithmetic coding compression technique.
9. If the size of WMI is not a multiple of 3, set all the bits of the LSB plane BP of WMI to zero to get a modified imageWMI1MOD.
10. Divide Watermarking image1MOD into N number of 3 × 3 non-overlapping blocks:IMb = {block imb(i, j),$1 \leq i, j \leq 3$}, where block imb(i, j) ∈ 0, 1, 2, . . ., 2L − 1
11. Obtain the final watermarked image WMI, by replacing the LSB plane BP of WMI1MOD by BLM. If the size of Watermarked image first is increased to get Watermarking image1MOD during watermark embedding, then reduce the size of Watermarking image to the original image size by removing the added rows and/or columns from WMI.

2.3. Watermarking Extraction

The Watermark extraction and verification process is used a salient steps can be numbered as follows:
Inputs: Watermarked and feasibly attacked image (WMI) of size P × Q.

1. Using the same function (as. WMEMB) used for watermark insertion, with proper key k(LSB); extract the bit should be representation of the embedded watermark, from the bit-plane BP of WMI. Let it be denoted by (*.mat file).
2. Divide mat file into two parts. One as the side information LSB bit stream (first 512 bits from mat file) and the rest as WMCOM (Decompression).
3. Decompress Watermark compression using arithmetic coding with the help of LSB (Data, Table and struct of Arithmetic Decompress) to WMCONCAT. Separate nv, v(x, y), IDX (Index of Bit stream), BP, LSB and OI-LSB get from WMCONCAT.
4. Replace the bits of the BP bit-planes in the ROI of WMI by the bits of BP bit plane and BP- Bit stream, respectively.
5. Extract the BP bit-plane of WMI.
6. Set all the bits of the BP bit-plane of WMI to 0 to get a modified image as WMIMOD.
7. Compute the binary location map (BLM) from the WMI.
8. To get the original Image(OI-Watermarked Image) and Secret Image (ROI Image).

III. RESULTS AND DISCUSSION

The proposed MIW technique was implemented in MATLAB. Experiments were done on a PC with 2.66 GHz CPU and 4 GB RAM. 430 medical images of 7 improved modalities (CT, MRI,USG, X-ray, Barium Study, Mammogram, etc.), manysizes, file formats (BMP, TIF, GIF, DICOM), and bit-depths (8,12, 16) were used to test our proposed method.

Among these 140 images were of size 512 ×512 pixels. Each of the 7 different modalities had 60 images individually. So, each modality of medical images consisted of 20 pictures of size 128 × 128, 256 × 256 and 512 ×512 pixels separately. The rest 10 images were DICOM images having changed sizes and bit-depths. EHR of different sizes were used in the experiments. Fig. 4 shows an example of the EHR used in the experiment.

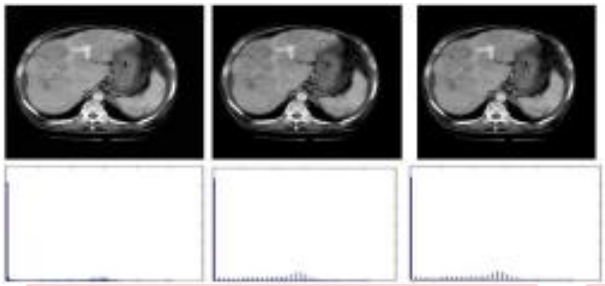
HISTOGRAM ANALYSIS

The histogram is a graphical representation of the distribution of numerical data. The vertical axis is not frequency but density: The number of gears per unit of the inconstant on the horizontal axis.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016



a) b) c)

Fig3: a) Original image b) Watermarked image c) Watermarked Extracted image

IV.CONCLUSION

Digital watermarking has been used all-in-one solution tool to address various issues about effective medical information.The blind, fragile watermarking system applied to medical images with good high consignment and better security. Our scheme can be used for changed modalities of medical images. It can be useful to a selection of digital health check images with different size, setup, and bit-depth. The tamper localization ability can effectively locate even a single tampered pixel and gives the conforming 3 × 3 block as the tampered region. The experimental results indicate that the medical image has been transferred successfully. It can be applied to the medical images at the time of acquisition, to serve many medical image application efficient controlled access retrieval and management.

REFERENCES

[1] Kannammal, K. Pavithra, S. Subha Rani (2012), "Double Watermarking of Dicom Medical Images using Wavelet DecompositionTechnique", European Journal of Scientific Research, Vol. 70, No. 1, pp. 46-55.

[2] Ankan Bhattacharya, SarbaniPalitNiveditaChatterjee, and Gourav Roy (2011), "Blind assessment of image quality employing fragile watermarking", 7th International Sym. on Image and Signal Processing and Analysis (ISPA 2011) Dubrovnik, Croatia, pp. 431-436.

[3] S. C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, pp. 417-420.

[4] Nisar Ahmed Memon, Asmatullahchaudhry and Mushtaq Ahmad, "Hybrid watermarking of medical images for ROI authentication and recovery", International Journal of Computer Mathematics, Vol.88, No.10, 2011, pp. 2057- 2071.

[5] X. Deng, Z. Chen, F. Zeng, Y. Zhang and Y. Mao, "Authentication and recovery of medical diagnostic image using dual reversible digital watermarking", Journal of Nanoscience and Nanotechnology, Vol. 13, No.3, 2013, pp. 2099-107.

[6] Hongxia Wang, Ke Ding, Changxing Liao (2008), "Chaotic Watermarking Scheme for Authenticationof JPEG Images", International Symposium on Biometrics and Security Technologies,pp. 1-4.

[7] YannFrauel, Albertina Castro, Thomas J. Naughton, and BahramJavidi, 'Resistance of the double random phase encryption against various attacks', Optical Society of America, 2007.

[8] Huang, J. and Shi, Y. Q., "Adaptive Image Watermarking Scheme Based on Visual masking," IEE Electronics Letters, Vol. 34, No. 8, pp. 748-750, 1998

[9] J. M. Zain and A. R. M. Fauzi, "Medical image watermarking with tamper detection and recovery", in Proceedings of the 28th IEEE EMBS Annual International Conference, 2006, pp. 3270-3273.

[10] S. C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, pp. 417-420.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

[11] S. C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery with Run Length Encoding compression", World Academy of -Science, Engineering and Technology, 2010, pp. 799-803