

# MEDICAL IMAGE BASED TAMPER AND REVERSIBLE WATERMARKING

AARTHY.R<sup>1</sup>, Dr.G.R.GNANA KING<sup>2</sup>,  
PG Scholar<sup>1</sup>, Associate Professor<sup>2</sup>,  
Kathir College of Engineering, Coimbatore.  
[aru93.ram@gmail.com](mailto:aru93.ram@gmail.com)<sup>1</sup>, [kings.326@gmail.com](mailto:kings.326@gmail.com)<sup>2</sup>

## ABSTRACT

Medical image plays very important role in clinical diagnosis. Now a day there is common practice of exchanging the medical images between hospitals located in different geographical area. This exchange of images takes place through insecure open networks like Internet which provides possibility of changes in medical image. We proposed the reversible watermarking scheme in medical image for tamper detection and recovery. Also the confidentiality of medical image is increased by embedding Electronic Patient Record (EPR) data. We used 800x600x8 bits ultrasound grayscale images in our experiment. However, medical images require extreme care when embedding additional data within them because the additional information must not affect the image quality which leads to wrong diagnosis. So image is divided into ROI (Region of Interest) and RONI (Region of Non Interest) parts.

Keywords: reversible, watermark, medical image, EPR, ROI, RONI

## INTRODUCTION

Scientific photo advantage digest consists of sufferer knowledge like patient title, sufferer-identity, ailment description, techniques with medical professionals knowledge [3]. Clinical image skills digest would be the watermark. This watermark is embedded into the picture which needs to be shared by using utilizing lossless watermarking manner. The info hiding scheme must have a significant embedding capability to hold more common knowledge. The goals of this work are to protect the copyrights and may get well the embedded information. The scheme offered right here for information embedding supplies robustness, imperceptibility, excessive embedding capacity and with ease retrieving potential. Clinical graphics can receive to the sufferer immediately or send to the sufferer by way of on-line and likewise maintained as a smooth and tough copy at the hospital for diagnosing and later someday functions. The crisis arises right here that's even as sending or giving the

data to the sufferer we need to in finding whether the info belongs to particular sufferers or no longer and also the privateness of the sufferer is a major obstacle [1]. Therefore authentication is required. If we take into account medical images in particular ultrasound and MRI, they are a personal property of the sufferers or defense personals and must be authenticated and transmitted without any vulnerable assault known as tempering. Nevertheless it's now not viable on this hacking discipline, so we ought to furnish some safety above all within the neighborhood of interest to prevent manipulations which outline the defected field of the patient. A number of ways are rising and watermarking is one among them. Some persons take watermarking as steganography but there's a difference between the two. Watermarking is defined because the practice of imperceptibly altering a work to embed a message about that work. However, steganography is to observe the undetectable altering an image to embed a secret message [2]. Digital

snapshot watermarking has gained an excellent interest within the last twenty years amongst students who provide a number of approaches. Nevertheless, still we are a long way far away from being totally or correctly triumphant. Hence, more and more folks are entering the area to make the watermarking inspiration priceless and trustworthy for the digital world. Of these more than a few watermarking methods, some beat others in phrases of basic watermarking specifications like robustness, invisibility, processing, rate and many others.

Watermarking approaches can by means of categorized into two categories, reversible and irreversible. The fundamental proposal at the back of reversible watermarking is to restrict irreversible distortion in fashioned image (the host image), with the aid of establishing approaches that may extract the original snapshot precisely. Scientific snapshot watermarking is one of the main fields that need such strategies the place distortion may just intent misdiagnosis [2]. Of course, the reversibly watermarked photograph shouldn't be distortion free, however that distorted photo is used as a carrier for data to be embedded and now not for prognosis. The losslessly recovered picture is the final one for analysis [3]. Although reversible schemes seem to be adequate for scientific photos, it ought to meet the entire requisites of scientific snapshot watermarking: imperceptibility, integrity manipulate, and authentication [4]. From the literature, the purposes of scientific photograph watermarking are categorized into two categories:

- 1- Tamper detection and authentication
- 2- EPR information hiding.

Tamper detection watermarks are equipped to locate the areas or pixels of the photograph where

tampering used to be carried out. Authentication watermarks are used to establish the source of the image. EPR knowledge hiding strategies provide extra significance in hiding excessive payload knowledge in the pix retaining the imperceptibility very high. Depending on the reason of the watermarking (tamper detection, authentication, or information hiding), a right watermarking procedure is chosen thus.

On this paper, we provide an overview of the earlier watermarking systems for clinical photographs. We then endorse a reversible ROI-founded watermarking scheme being ready of hiding sufferer's knowledge, verifying authenticity of ROI, localize tampered areas, and get better those tampered areas within ROI. In section II, we evaluate watermarking approaches proposed for scientific pics. In section III, we gift our watermarking scheme, together with information embedding, extracting, verifying, tamper localization and healing. In section IV, experimental results are offered to illustrate the efficiency of the scheme. Subsequently, in part V we present our conclusion.

#### **RELATED WORKS**

Any watermarking schemes were proposed for clinical photographs. Those systems may also be spatial domain procedures [5]-[9], frequency domain method, or a blend of the two domains. An LSB-centered reversible scheme was proposed by using Zain et al. For ultrasound pictures, where the usual photo can be recovered utterly [5],[6]. In embedding process, an SHA-256 hash code is calculated for the ROI chosen. After that, the hash code is embedded into the LSB of RONI. The reversibility of the scheme situated on the fact that the common values of RONI pixels had been zeros earlier than

embedding, at the receiver finish, the watermark is extracted from LSB's of RONI and those pixels which carried the watermark are reset again to zero. This may occasionally produce the usual photo earlier than embedding watermark. The authentication is performed by using comparing the extracted hash values with the hash values of the extracted picture. If they are the same, then the photo is authentic.

An extra spatial area process was once proposed through Zain et al. To strengthen the security of clinical portraits by means of involving the capability to become aware of tamper and subsequently recuperate the photo [7]. The scheme requires a secret key and a public chaotic mixing algorithm combined with simple operations such parity assess and compression to embed and get well a tampered image. In embedding process, the image is divided into blocks of 8x8 pixels each and every. For each and every block B, we further divide it into four sub-blocks of 4x4 pixels. The watermark, which is embedded utilizing LSB's, in every sub block is a 3-tuple (v, p, r), the place both v and p are 1-bit authentication watermark, and r is a 7-bit healing watermark for the corresponding sub-block inside block A mapped to B utilizing a mapping operate. For the duration of extraction, v and p are used for tamper detection and localization. This scheme was once modified by Zain et al. By means of divide ROI and RONI into smaller blocks [8]. Besides, the authentication bits, v & p, are embedded into sub blocks of ROI, whilst the 7-bits recovery knowledge are embedded into the corresponding sub blocks of RONI. This may occasionally support the picture

excellent in ROI because the highest trade is simplest 2 bits in every four pixels.

Raul et al. Adopted picture second thought to normalize the photograph as a way to acquire a strong watermarking scheme against lively assaults equivalent to filtering, compression, and geometrical assaults [9]. Embedding watermark is done in areas with low homogeneity, which may also be obtained by scanning the snapshot in a spiral way utilizing the centroid as the foundation of this scan.

For the duration of extracting segment, the photo is scanned in the identical spiral approach opening from the centroid of the photograph. Somewhat of the watermark is extracted from an area by way of comparing the gray scale level of the center pixel with the grey scale degree imply of the neighborhood.

A fingerprint mannequin suitable for many-to-many multicast used to be proposed by Li et al. The mannequin is computationally effective and scalable in user storage and communicate. The major goal of their scheme is tracing the supply of an unauthorized free up of medical pics to enhance patient's privacy. So as to develop the robustness of their scheme, they adopted an snapshot adaptive scheme established on wavelet (IAW). A four stage IA Wavelet scheme is used as the underlying watermarking scheme. The watermark is inserted into LH and HL band of degree two and 4 wavelet decompositions.

For tamper detection and restoration functions, two schemes founded on Modulo 256 and DCT used to be proposed by using Wu et al. In the beginning, the photograph is split into a couple of blocks, and for every block, an adaptive strong digital watermarking method combined with the modulo operation is used

to hide the watermark. Within the first scheme, each and every block is embedded with the watermark, which is a combination of an authentication message (hash value of the block) and the healing expertise of alternative blocks. Seeing that the recovered block is simply too small and excessively compressed, the concept of vicinity of curiosity (ROI) is offered into the 2nd scheme. The JPEG bits of ROI are mixed with hash worth to type the watermark, and the watermark is embedded into ROI simplest. If there aren't any tampered blocks, the long-established photograph will also be got with simplest the stego snapshot. When the ROI is tampered with, an approximate photograph will probably be bought from different blocks.

Woo et al. Proposed a couple of digital picture watermarking procedure which is compatible for privacy manage and tamper detection in scientific pictures. The a couple of watermarks consist of an annotation watermark, and a fragile watermark, which will notice normal photograph manipulations akin to photo compression, noise insertion, and duplicate attack. In embedding approach, the annotation watermark is embedded into the border pixels of the photo utilizing a robust embedding method. The watermark message is embedded making use of a linear additive method into the three excessive cross bands (HL1, LH1, & HH1) of DWT of the common photograph borders. The fragile watermark, which is a binary watermark pattern is tiled to cover the entire image, is embedded into the relevant neighborhood of the usual image making use of the least significant bit (LSB) procedure.

A lossless scheme was proposed by using Guo et al. Founded on difference growth offered via Tian. The scheme used to be proposed to beat a few of dangers of Tian's customary scheme, that are the overhead of retaining a place map, which influence the hiding capacity, and the distortion brought on by embedding watermark bits. To overcome these drawbacks, they adopted difference enlargement technique to preclude the embedded-triggered distortion within a given vicinity and controlling the embedding capability. The area of embedding (ROE) is chosen to preclude introducing any distortion within the ROI. Alternatively of increasing the difference between two adjoining pixels, the scheme is centered on increasing the difference between 4 pixels as a quad. Three bits of the watermark are embedded into each expandable quad. The watermark includes a hash value and patient's data.

Two reversible schemes based on DE technique were proposed by way of Chiang et al. For tamper detection and restoration. Within the two schemes proposed, the picture is divided into blocks of 4x4 each, and each block is transformed making use of 2-degree DE manner. Best smooth blocks, with equal pixel values, are used for embedding watermark. Within the first scheme, the usual of each block is calculated and concatenated collectively to type the watermark, which is used as recovery understanding. The 2nd scheme is a ROI-based scheme, and the pixel values of ROI is used as the watermark with the intention to recuperation the unique ROI in case of tampering. The predicament of this manner is the constrained ability due to the fact simplest tender blocks are used for embedding, so that it can not be used for all photograph modalities.

**DESIGN**

The design of this watermarking scheme proposed in [9] in terms of watermark embedding, tamper detection and healing. Extra developments were made in photograph instruction, embedding and storing usual bits to permit this watermarking scheme to be reversible. RLE as an information compression process is used to achieve greater embedding capacity.

**A. Image training**

Image training the important thing for this scheme to be reversible. An extra process is taken by means of dividing a 640x480 pixels ultrasound snapshot into ROI and RONI as proven in Fig. 1.



Fig. 1 Ultrasound image divided into ROI and RONI

Our proposed system can be utilized for hiding patient's information, authenticating ROI, localizing tampered areas within ROI, and recuperating those tampered areas when wanted. The block diagram for encryption and decryption process is shown in figure 2 and figure 3.

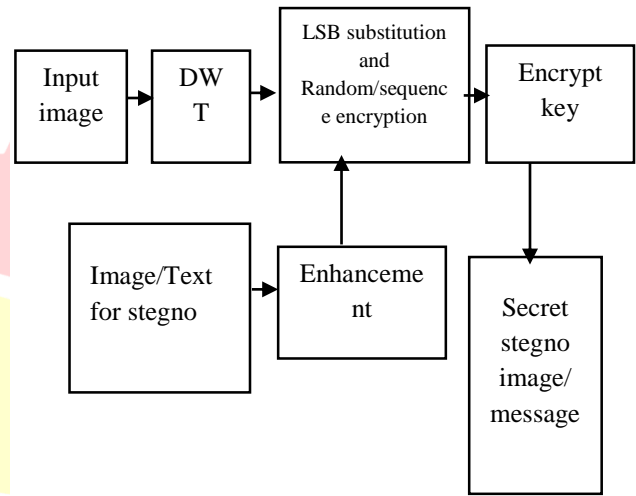


Figure 2 Encryption process

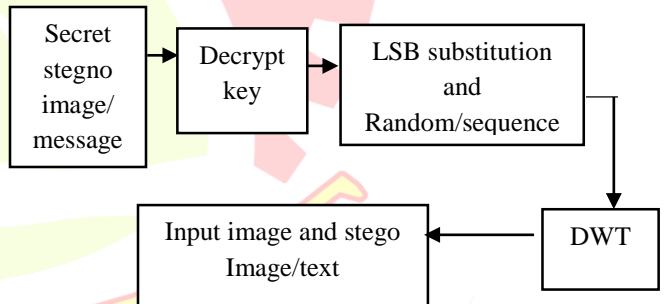


Figure 3 Decryption process

Additionally, the normal photograph is recovered precisely after watermark extraction on the receiver end. The system divides the photo into three areas, ROI, RONI, and the border. The payload is embedded into RONI using 2d-DE scheme, and this produces an embedding map as a way to be used later for the period of extraction section. The embedding map is embedded into LSB's of border pixels. The payload consists of:

1. Sufferer's information.



2. Hash message of ROI; which will be used to authenticate ROI.

Three. ROI pixels; so that it will be used for tamper detection and recuperation when wanted.

4. LSB's of border pixels, so that they can be used to restore the common border pixels.

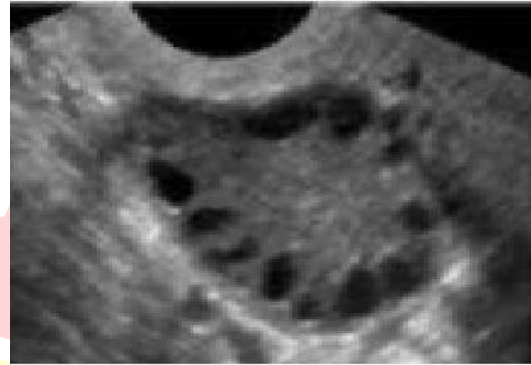


Figure 4. Image for testing 800\*6\*88

#### A. The embedding phase:

1- ROI is chosen and the RONI and the border areas are outlined.

2- ROI is divided into blocks of 16 x 16 pixels.

Three- The hash message for ROI, H, is calculated making use of MD5 algorithm.

Four- The bits of ROI pixels are amassed as P.

5- The LSB's of border's pixels are gathered as L.

6- The sufferer's knowledge, D, is concatenated with H, P, and L and then compressed utilizing Huffman coding to the shape the payload.

7- The payload is embedded into RONI using 2DDE scheme stated above, and the embedding map is generated.

Eight- The embedding map is concatenated with ROI coordinates, compressed, after which embedded into LSB's of border's pixels. The watermarked photo is now able to be stored in the clinic's database procedure or will also be dispatched to a different clinical tuition.

#### B. The extracting phase

1- The LSB's of the border's pixels are accrued. The accrued bit stream is depressed and the embedding map is generated and ROI coordinates are extracted.

2- utilizing ROI coordinates; ROI and RONI areas are outlined.

Three- The payload is extracted from RONI, decompressed, after which decomposed to the five materials; H, P, L, D.

Four- The hash message of ROI is calculated and compared to the extracted one. If they are equal, the image is said to be reliable and proceed to step 6. If not, the photo is just not reliable, and which means some tampering is detected. In the next step the tampered discipline is localized and recovered.

5- ROI is split into blocks of sixteen x sixteen pixels. The usual worth of each and every block is calculated and compared to value of the average of the corresponding pixel in the extracted ROI; P. If they are not equal, the block is marked as tampered and changed by using the corresponding pixels P.

6- The LSB's of the border's pixels are recovered utilizing the bits of L.

**RESULT AND DISCUSSION**

The experimental results are discussed for the given EPR medical image of 800\*600\*8 bit ultrasound grayscale image. The input image is shown in above figure 4. The preprocessing techniques used for input image is shown in figure 5.

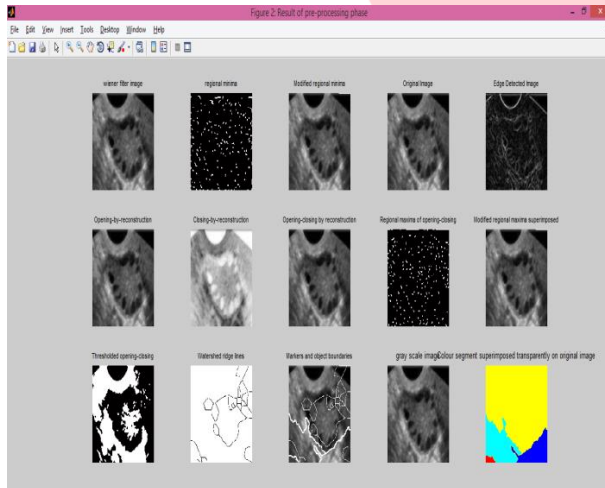
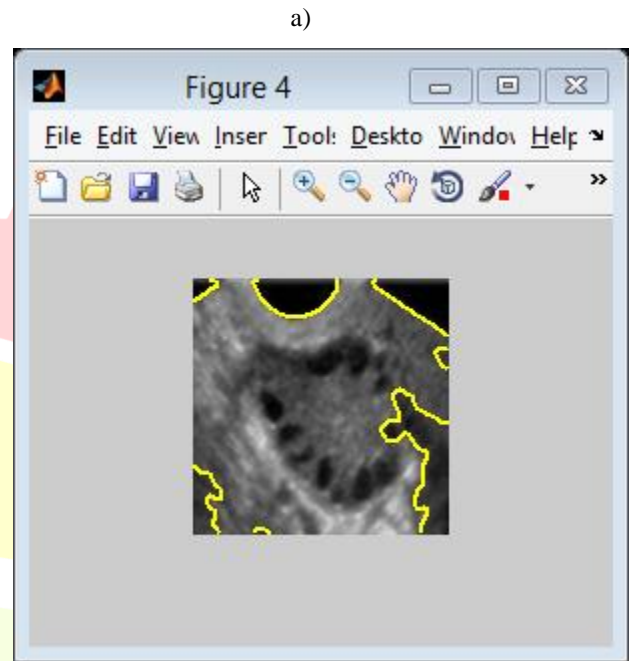
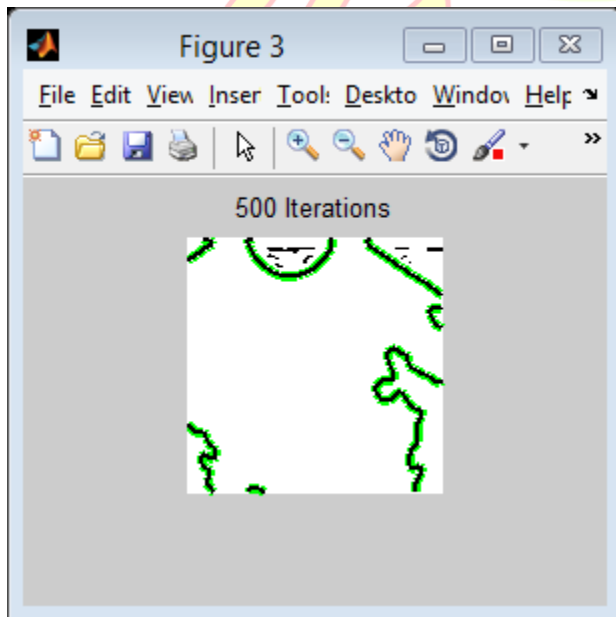


Figure 5 Preprocessing

The region of interest for the iteration of the image to divide into 16\*16 block as shown in figure 6 a) and b)



b)

Figure 6 a) ROI iteration  
 b) ROI region

The histogram modification for the ROI image as block 1 and block 2 is shown in figure 7.

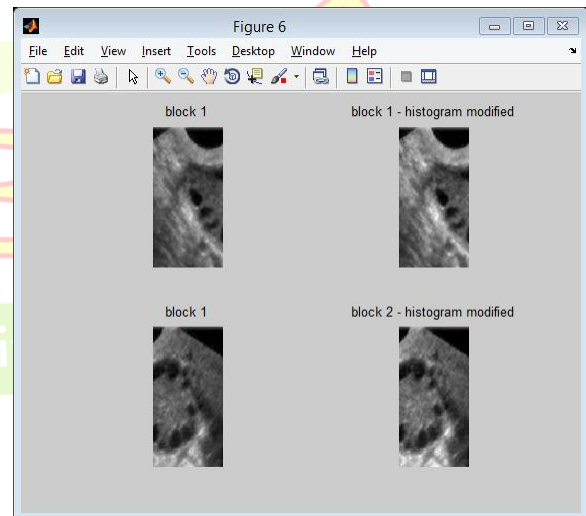
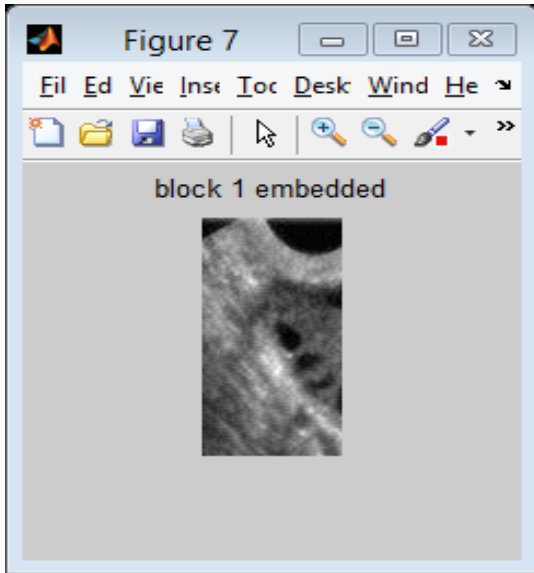
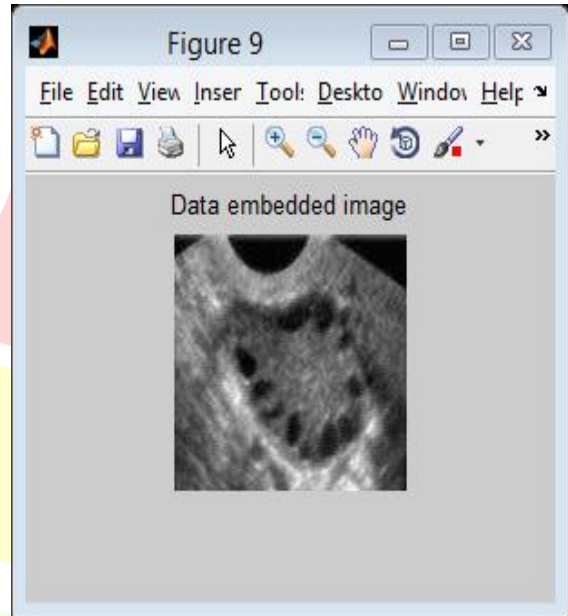


Figure 7 Histogram Modified image

The Block 1 and Block 2 encryption of image with the message and encrypted image is shown in figure 8.

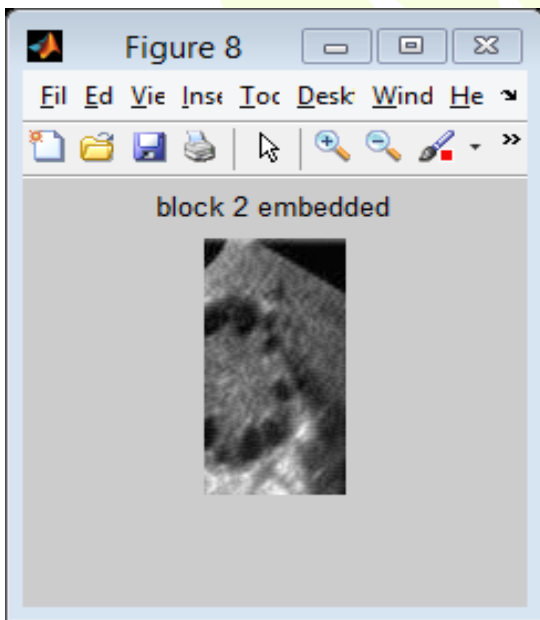


a)

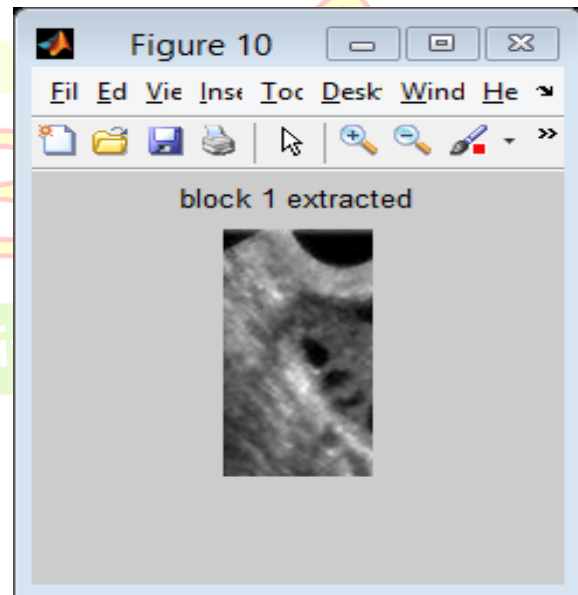


c)

Figure 8 a) Block 1 b) Block 2 c) Embedded image

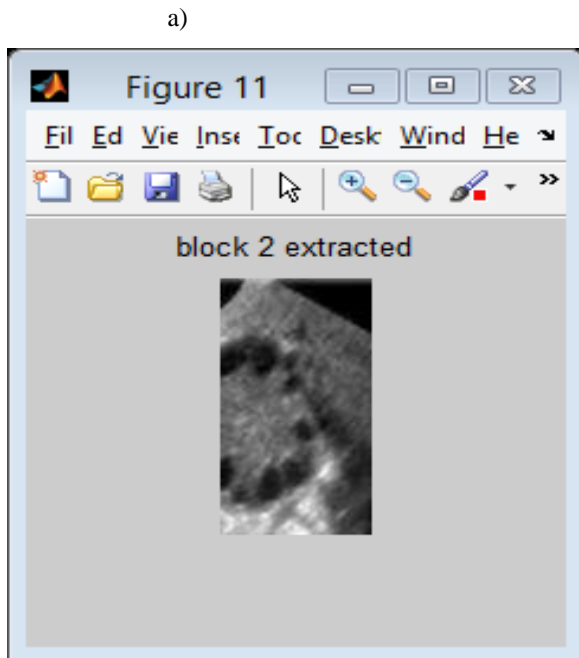


b)



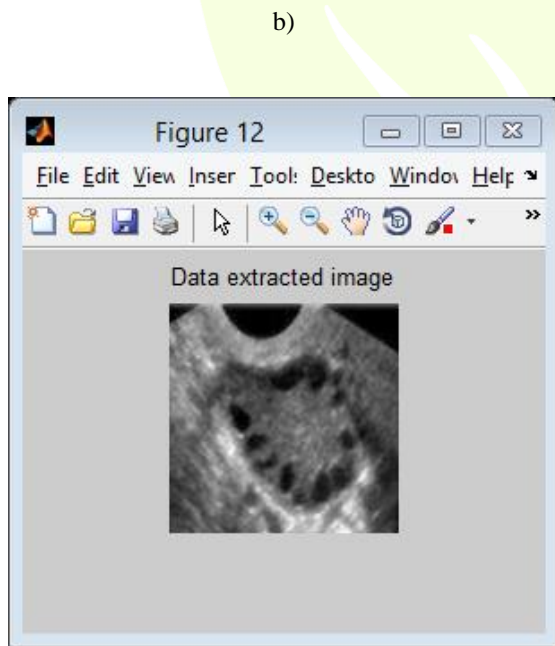
The Block 1 and Block 2 decryption of image with the message and encrypted image is shown in figure 9.





```
Command Window
psnr =
    57.4077
mse =
    0.1181
str =
    Welcometokathir
str1 =
    AppliedElectronics
```

Figure 10 PSNR, MSE and Data extracted



c)

Figure 9 a) Block 1 b) Block 2 c) Data extracted image

The Peak signal to noise ratio (PSNR), Mean Square Error (MSE) for the image calculated is shown in figure 10.

### CONCLUSION

EPR knowledge hiding utilizing classification stylish Coding Scheme can be used as mighty coding scheme for hiding information in medical pix which supplies higher perceptual first-class of stego photograph together with develop in embedding ability.

This process enhances the robustness towards quite a lot of assaults like JPEG compression, snapshot tampering and photograph manipulation. This manner additionally provides flexibility to doctors in settling on the critical discipline of the scientific picture as ROI. Also any tamper within the ROI can also be conveniently detected. If lossless compression is utilized on stegno photograph and the stegno photo isn't altered earlier than authentication, then hidden data, common picture as well as hash bits can also be extracted safely. Else if compression just isn't so extreme then hidden data may also be extracted accurately however customary snapshot can't be recovered. So this process even though provide excessive knowledge hiding potential however robustness in opposition to intentional assaults is affordable.

Reversible data hiding utilizing 2-dimensional change enlargement process can be used for hiding information in significant quantity and furnish authenticity to medical photos. This procedure no longer handiest detects the locations of tampered areas within ROI of watermarked scientific photographs but also recuperate the contents of tampered areas. Very good performance is carried out within the terms of hiding capacity and visual best using this procedure.

Reversible watermarking using pixel change and histogram transferring offered the thought of binary tree which predetermines the a couple of peak facets used to embed messages hence, the only information sender and recipient need to share is tree stage L, removing the need for facet conversation channel for transferring pairs of height and minimum facets between sender and receiver. As this procedure is centered on pixel difference, it makes it possible for to gain significant hiding capability whilst maintaining embedding distortion low because of excessive correlation and spatial redundancy between neighbor pixels.

#### REFERENCES

- [1] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Digital watermarking, (Morgan Kaufmann Publishers, 340 Pine Street, Sixth floor, Sans Francisco, CA, USA, 2004)
- [2] Rajendra Acharya U., U. C. Niranjana, S.S. Iyengar, N. Kannathal, Lim Choo Min “Simultaneous storage of patient information with medical images in the frequency domain, Computer Methods and Programs in Biomedicine, Vol. 76, 2004, pp.13-19.
- [3] H. Munch, U. Englemann, A. Schroter, H.P. Meinzer “The integration of medical images with the patient record and their web based distribution” Journal of Academic Radiology, 11(6), June 2004, 1995, pp.661-668.
- [4] Rajendra Acharya U., P. Subhanna Bhat, Sathish Kumar, Lim Choo Min, Transmission and storage of medical images with patient information, Journal of Computers in Biology and Medicine, 33, 2003, pp.303-310.
- [5] Akiyoshi Wakatani, Digital watermarking for ROI medical images by using compressed signature image” Proc. of the 35<sup>th</sup> Int. Conference on System Sciences-2002.
- [6] Hui-Mei chao, Chin-Ming Hsu, Ahaou-Gang Miaou, A data hiding technique with authentication, integration and confidentiality for electronic patient records, IEEE trans. Inf. Tech. in biomedicine, 6(1), March 2002, 46-53
- [7] Dan Yu, Farook Sathar, Kai-Kuang Ma Watermark detection and extraction using independent component analysis, EURASIP J. on Applied Signal Processing 2002, 92-104.
- [8] Jasni M. Zain, L.P Balwin, M. Clarke,” Reversible watermarking for authentication of DICOM images”, in Proc. 26th Annual International Conference of the IEEE EMBS, San Francisco, USA Sep 2004, pp. 3237 - 3240, ISBN: 0-7803-8439-3.
- [9] Jasni M. Zain, Abdul R.M. Fauzi, “Medical Image Watermarking with Tamper Detection and Recovery”, in Proc. 28th Annual International Conference of the IEEE EMBS, New York, USA, Sept. 2006, pp. 3270- 3273, doi: 10.1109/IEMBS.2006.260767.

- [10] Chang, Chin-Chen, Lin, Chih-Yang, Wang, Yu-Zheng , "New image steganographic methods using run-length approach", Information Sciences, Volume 176, Issue 22, 22 November 2006, Pages 3393-3408, ISSN 0020-0255, doi: 10.1016/j.ins.2006.02.008.
- [11] Lin ,Rey-Sern, Hu,Shang-Wen, "A Modified Run-length Image Data Hiding for High Embedding Capacity," Information Assurance and Security, International Symposium on, Fifth International Conference on Information Assurance and Security,2009, pp. 673-676, doi: 10.1109/IAS.2009.35.

