Efficient Medical Image watermarking with Tamper Detection and Recovery

Kusuma Prabhu
M.Tech student, Dept. of E&C,
NMAMIT, Nitte, Udupi, India
kusum.prabhu@gmail.com

Raksha
M.Tech student, Dept of E&C,
NMAMIT, Nitte, Udupi, India
raksha.s20@gmail.com

***Abstract*—A block-wise and content-based medical image authentication scheme with location and recovery is presented. This paper presents authenticity and integrity of medical images using watermarking. In this section a case of using intensity average comparisons and parity bits as the authentication watermark is presented. To localize tamper in a block, the watermark needs to be embedded directly into that block. If a block is being tampered locally, the intensities of the pixels involved will be changed. This will also change the average intensity of the block concerned. To ensure that this is not changed, a parity check will be used. However, a parity check alone will not guarantee that the block has not been changed. To overcome this, the intensity comparison is used as another guard. Watermarking should also serve as an integrity control and should be able to authenticate the medical image Authentication Watermarking with Tamper Detection and Recovery is able to localize tampering, while simultaneously reconstructing the original image.**

Keywords—medical imaging, integrity control, watermarking

I. INTRODUCTION

Medical Images such as radiographs, ultra sound and magnetic resonance images play important part in the process of diagnosing a patient by medical practitioners. Advancement in the medical information system is changing in the way patient records are stored, accessed and distributed. Medical images can be stored in the digital form temporarily or permanently on a server along with patient records. Malicious tampering of medical image for the purpose of Insurance claims or to hide a medical condition for personal gain is possible. The integrity of the medical images and their information needs to be protected from unauthorized modification or destruction. The current security measures used to protect integrity of the patient records are such as VPN (Virtual Private Network, Data encryption, Data embedding. It is vital to keep images safe from any damage, it is also important being able to detect when an image has been modified. Indeed, medical images can be modified accidentally, for example during their transmission, or deliberately. In this latter case, images can be tampered with the introduction or the removal of lesions. Also, it must be known that some image processing may lead to similar situations. In telemedicine applications, for instance, lossy image compression is tolerated so as to reduce the amount of information to be transmitted. However, depending on its extent, this process may induce unacceptable information loss and results in a misdiagnosis, involving at the same time liabilities of physicians.

In this section, an efficient and effective digital watermarking method for image tamper detection and recovery is presented. The method is based on four concepts introduced from the literature: 1) block-based Fridrich et al.[1] 2) Separating authentication bits and recovery bits Lin et al[2]. 3) Hierarchical Celik et al [3] and Average intensity as an image feature Lou et al[4]. The method is efficient as it only uses simple operations such as parity check and comparison between average intensities. It is effective because the scheme inspects the image hierarchically with the inspection view increasing along with the hierarchy so that the accuracy of tamper localization can be ensured. This scheme can perform both tamper detection and recovery for tampered images. Tamper detection is achieved through a block-based, inspection and recovery of a tampered block and relies on its feature information hidden in another block, which can be determined by a one-dimensional transformation.

II. THE PROPOSED AUTHENTICATION METHOD

LSB is suggested, to minimize the degradation as medical images are very strict with the quality. The recovered image, however, will not be considered authentic and will not be used for any clinical purposes. One possibility for the purpose of recovery is to help in the investigation to find the motive and the person responsible for the tampering. A 3x3 sub block in a 6x6 block is suggested to accommodate two authentication bits and seven recovery bits to be embedded in the LSB of each pixel.

A. Embedding

For each block B of 6x6 pixels, divide it into four sub-blocks of 3x3 pixels. The watermark in each sub-block is a 3-tuple (v, p, r), where both v and p are 1-bit authentication watermark, and r is a 7-bit recovery watermark for the corresponding sub-block within block A mapped to B. The following algorithm describes how the 3-tuple watermark of each sub-block is generated and embedded which is described in fig 1 and fig 2.

1. Set the LSB of each pixel within the block to zero and compute the average intensity of the block and each of its four sub-blocks, denoted by avg_B and avg_Bs, respectively.

2. Generate the authentication watermark, v, of each sub- block as:

$$v = \begin{cases} 1 & \text{if } avg\_Bs \geq avg\_B \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

3. Generate the parity check bit, p, of each sub-block as

$$p = \begin{cases} 1 & \text{if number is odd,} \\ 0 & \text{Otherwise} \end{cases} \quad (2)$$

Where, num is the total number of 1s in the seven MSBs of avg_B_s.

4. From the mapping sequence generated in the preparation step, obtain block A whose recovery information will be stored in block B.
5. Compute the average intensity of each corresponding sub-block A_s within A, and denote it avg_A_s.
6. Obtain the recovery intensity, r, of A_s by taking the seven MSBs in avg_A_s.
7. Embed the 3-tuple watermark (v, p, r), 9 bits in all, onto the LSB of each pixel in B_s.

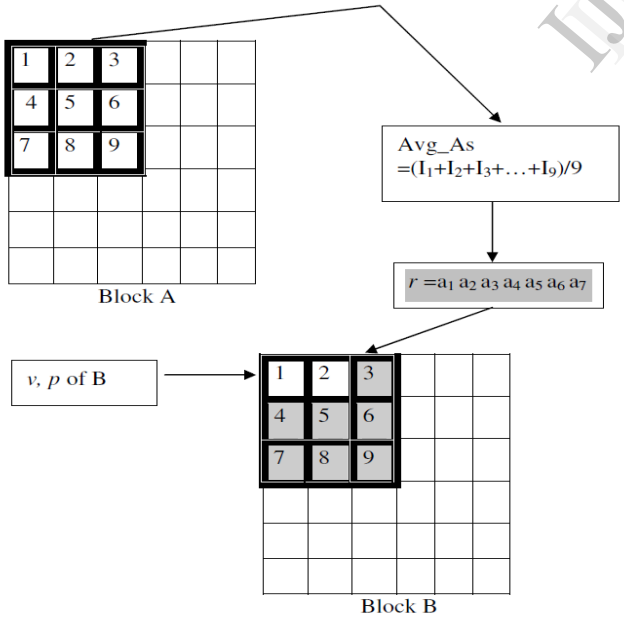


Fig 1 Watermark generation and embedding location

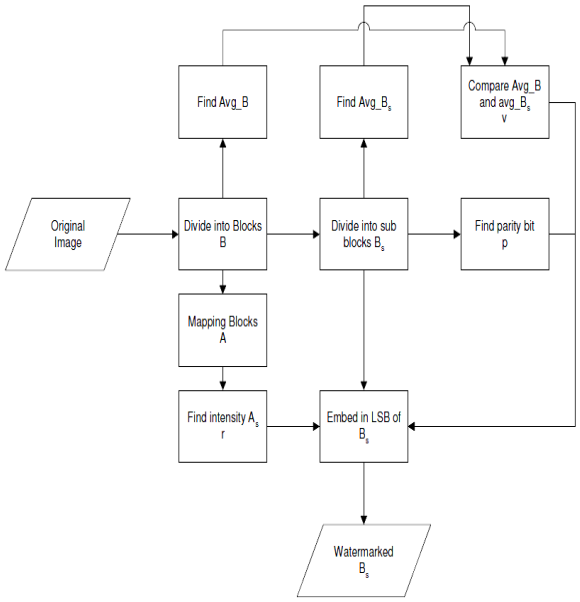


Fig 2 AW-TDR embedding scheme

B. Tamper detection

The test image is first divided into non-overlapping blocks of 6x6 pixels, as in the watermarking embedding process. For each block denoted as Br, the LSBs of each pixel in Br were set to zero and compute its average intensity, denoted as avg_B_r. A 2-level detection is then performed. In level-1 detection, each 3x3 sub-block within one block is examined. In level-2 detection, a 6x6 block is treated as one unit. Level-3 detection is for VQ attack resilience only. The procedure of our hierarchical tamper detection scheme is described in the following:

1). Level-1 detection.

For each sub-block B_{rs} of 3x3 pixels within the block B_r, perform the following steps:

1. Extract v and p from B_{rs}.
2. Set the LSBs of each pixel within each B_{rs} to zero and compute the average intensity for each sub-block B_{rs}, denoted as avg_B_{rs}.
3. Count the total number of 1s in avg_B_{rs} and denote it as P_s.
4. Set the parity check bit p' of B_{rs} to 1 if P_s is odd, otherwise, set it to 0.
5. Compare p' with p. If they are not equal, mark B_{rs} as tampered and complete the detection for B_{rs}.
6. Set the algebraic relation v'=1if $avg\_B_{rs} >= avg\_B_r$, otherwise, set it to 0. 7. Compare v' with v. If they are not equal, mark Brs as tampered and complete the detection for Brs; otherwise mark it as valid.

2). Level-2 detection.

For each block of size 6x6 pixels, mark this block tampered if any of its sub-blocks is marked tampered; otherwise mark it valid.

3). Level-3 detection

For each valid block Br of size 6x6 pixels, perform the following steps:

1. Find the block number of block C, where block C is the one in which the intensity feature of block B_r is embedded.
2. Locate block C.
3. If block C is marked tampered, assume block B_r is valid and complete the test.
4. If block C is valid, perform the following steps:

Obtain the 7-bit should-be intensity of each B_{rs} by extracting the LSBs from each pixels in the corresponding block within block C, padding one zero to the end to make an 8-bit value.

Compare with avg_B_{rs} and mark B_r tampered if they are different.

C. Image Recovery

After the detection stage, all the blocks are marked either valid or tampered. Only the tampered blocks are recovered and the valid blocks are left as they are. For convenience, we call the tampered block, block B and the block embedded with its intensity, block C. The restoration procedure for each tampered block is described as follows:

1. Calculate the block number for block C.
2. Locate block C.
3. Obtain the 7-bit intensity of each sub-block within block B, padding one zero to the end to make an 8-bit value.
4. Replace the new intensity of each pixel within the sub-block with this new 8-bit intensity.
5. Repeat step 3 and 4 for all sub-blocks within block B.

III. EXPERIMENTAL RESULTS

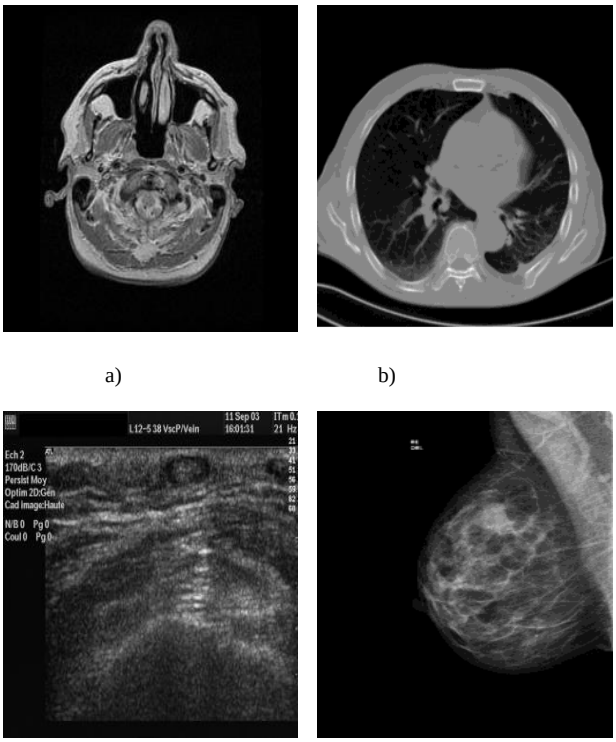
The localization accuracy and recovery correctness were tested by making various modifications to the watermarked image.

Different image modularity's have been considered:

-Magnetic resonance (MRI) of head 256× 256 pixels

-X-Ray imaging: Mammograms of 256× 256 pixels

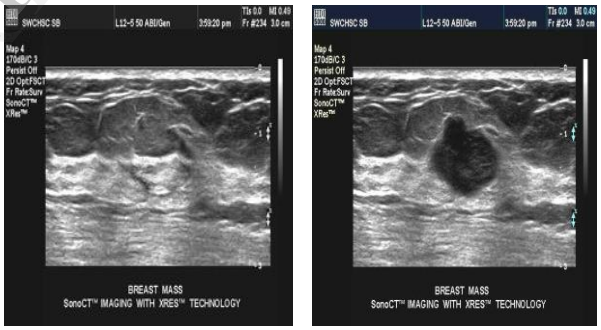
-Ultra sound imaging: Echo of vein 256× 256 pixels



a) b)

c) d)

Fig. 3 Samples of our experimental image data sets

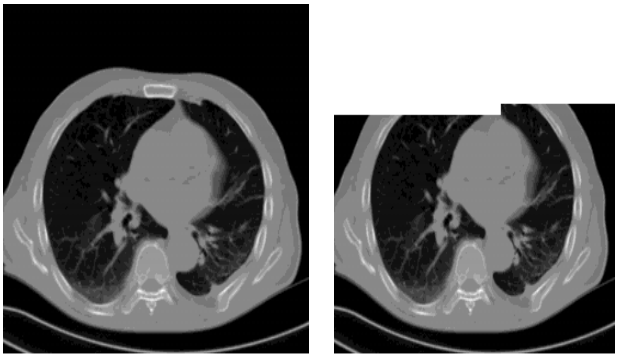


a) b)

c)

Fig 4.a. Watermarked image b. Tampered image
c. Recovered image

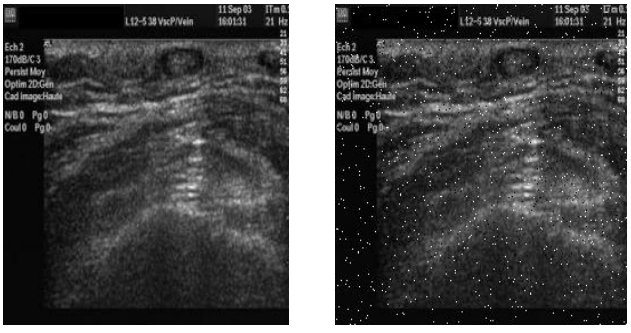
In Fig 4.b.The cyst was removed from the image by using the healing brush tool. If this image were a critical piece of evidence in a legal case or police investigation, this form of tampering might pose a serious problem.



a) b)

c)

Fig 5. a. Watermarked image b. Spread tampered image
c. Recovered image



a) b)

c)

Fig 6. a. Watermark image b. Salt &Pepper attack
c. Recovered image

When, Salt & Pepper noise is added in the medical image at 3% as in Fig 5.b and when image undergoes spread tampering as in Fig 6.b, the results show that our proposed algorithm has strong robustness against noise and spread tampering attacks.

TABLE 1

The PSNR and MSE of the recovered image

Image Processing	**Image samples**	**PSNR**	**MSE**
Gaussian noise	1)MRI 2)CT image 3)X-Ray image 4)Echo grapy	31.4383 30.8477 30.3237 31.3782	46.6927 53.4952 60.3542 47.3437
Salt& pepper	1)MRI 2)CT image 3)X-Ray image 4)Echo grapy	20.9616 21.4124 21.7671 20.7730	521.0980 469.7250 432.8821 544.2255
Median filtering	1)MRI 2)CT image 3)X-Ray image 4)Echo grapy	31.5257 33.8241 27.3453 35.9756	45.7626 26.9570 119.8254 16.4255
Spread tampering (10%)	1)MRI 2)CT image 3)X-Ray image 4)Echo grapy	38.12 34.62 31.31 28.98	4.28 10.85 13.61 15.93
No attack	1)MRI 2)CT image 3)X-Ray image 4)Echo grapy	54.3024 53.4093 53.6550 55.3088	0.2415 0.2966 0.2803 0.1915

IV.CONCLUSIONS

In this paper we proposed a watermarking scheme that can detect and localize tamper and recover the images. The purpose is to verify the integrity and authenticity of images. We presented our watermarking procedures that include data embedding, tamper detection and recovery procedure. The experimental results demonstrate that the precision of tamper detection and localization is close to 100% after level-2 detection. The tamper recovery rate is better than 86% for a less than half a tampered image.

REFERENCES

[1] Fridrich, J. and Goljan, M., 1999. "Images with self-correcting capabilities", IEEE International Conference on Image Processing, 3, pp. 792-796.

[2] Lin, C and Chang, S 2001."A robust image authentication method distinguishing JPEG compression from malicious manipulation", IEEE Transactions on Circuits and Systems for Video Technology, 11(2), pp. 153-168.

[3] Celik, M.U., Sharma, G., Tekalp, A.M., 2002. "Hierarchical watermarking for secure image authentication with localization", IEEE Transactions on Image Processing, 11(6), pp.585-594.

[4] Lou, D. C. and Liu, J. L., 2000. "Fault resilient and compression tolerant digital signature for image authentication". IEEE Transactions on Consumer Electronics, 46(1), pp. 31-39.

[5] H.-J. He, J.-S. Zhang, and H.-M. Tai, "Self-recovery Fragile Watermarking Using Block-Neighborhood Tampering Characterization," in Proc. Information Hiding, 2009, pp. 132-145.

[6] Phen-Lan Lin, Po-Whei Huang, An-Wei Peng, "A Fragile Watermarking Scheme for Image Authentication with Localization and Recover," Multimedia Software Engineering, 2004. Proceedings. IEEE Sixth International Symposium on 13-15 Dec. 2004.