REVERSIBLE MEDICAL IMAGE WATERMARKING TECHNIQUE USING HISTOGRAM SHIFTING

S.Mounika[1], M.L. Mittal[2]

[1]*Department of ECE, MRCET, Hyderabad, India*
[2] *Professor Department of ECE, MRCET, Hyderabad, India*

ABSTRACT

With the development of information technique, the power of image processing software become stronger, and we can edit the digital images more easily. So the copyright protection, the integrity authentication of digital image becomes an urgent issue. At the same time, the rapid development of medical technique, there are more and more digital images, and they need be preserved, transmitted, an so on. However, the copyright of it should be researched. And the contents of digital medical images contain more important information, and any change of it may result in physiotherapy accident. How to authenticate the digital images' reality and integrity become so important that we should use new technique to protect them. Digital watermarking is a technique that embeds important data into host multimedia, and it can be used in digital right management, authentication and data hiding. In this paper, we will analyze the character of medical images and watermarking technique. And give the basic procedure of them, and analyze the performance of these algorithms.

Keywords: Authentication, Data Hiding, Digital Right Management, Digital Watermarking; Medical Images.

I. INTRODUCTION

The development of medical technique, three are more and more digital medical images. The management of these digital medical images becomes a big problem. Firstly, the medical images should be transmitted on line for need of research of medical technique. However, the illegal user may want to pocket them for some benefit. So, how to protect the copyright right of them should be researched. Secondly, the important content of digital medical images implies that any change of the digital medical images will result to big physiotherapy accident. For example, doctor can charge the illness due to the distribution of nerve in digital eye-ground images. And if the detail information for digital eye-ground image has been edited by illegal user using image software, the doctor may think that there are something wrong with the patient, and do a operation. And this misdiagnosis may make the patient lose life. Therefore, we should authenticate the reality and the integrity of the medical images. Thirdly, the increasing amount of digital medical images makes the preservation of auxiliary information, such as the patient' name, the diagnosis information, and so on, be a problem. Sometimes, the loss of auxiliary information, or the non-match of auxiliary information and digital images may bring danger to patients. If we embed the auxiliary information into the digital images, and we extract it when we use it, the auxiliary information and digital images will match well all the time.

In summary, the copyrights protection, the reality and integrity authentication and data hiding of digital medical images should be solved. Digital image watermarking [1-19] embeds useful information into the protected image, and the information can include copyright information, the authentication code, or auxiliary information. And the copyright information may be a tag or ownership identifier that prevents the illegal users utilizing the image to make an error. And the authentication code can use the cover's character to test that the digital images are real or not. Meanwhile, data hiding in watermarking algorithm can hide the useful information into digital images, and these information will assist preserve some easily lost information. And all of these functions can be used in digital medical images. In this paper, we will discuss the watermarking technique for digital medical images from three aspects, and they are copyright protection, integrity authentication and data hiding. This paper will be structured as follows; In Section II we will analyze the basic procedure of digital watermarking algorithm for copyright; In Section III, the two types of authentication algorithm named non-recovery authentication algorithm and self-recovery authentication algorithm are given. Subsequently, we will describe the Data hiding algorithm in section IV. Finally, we draw our conclusions in section V.

II. COPYRIGHT PROTECTIONS

Watermarking algorithm for copyright protection embed copyright information into protected images, for example, the logo. For digital medical images, we can embed the patient's name, or the hospital's name, and so on. When need to verify the copyright, the embedded information is extracted. Algorithms for copyright protection can be classified as different types. For example, the algorithm can be classified as spatial algorithms, transform algorithm, or compressed algorithm by the embedding domain. In this paper, we divide the algorithms into two big types: non-visible watermarking algorithm and visible watermarking algorithm due to that the embedded watermark is visible or not

2.1. Non-visible Watermarking Algorithm

Watermarking algorithm area is focus on visible watermarking and watermark in these algorithms isn't recognized by naked eyes, so these algorithms have high quality. The basic embedding procedure of non-visible watermarking algorithm is like 1. Firstly, the funcI means the key generator which can select the embedding position. And the fuc2 means the embedding algorithm. We may use the human visual system to decide the embedding strength when embed the watermark image into the cover image. From figure 1, we can find that the non-visible watermarked digital medical image has no obvious difference with the original digital medical image in vision.

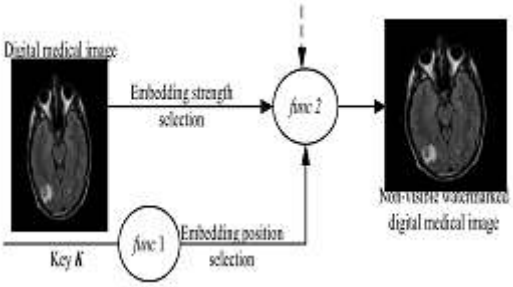


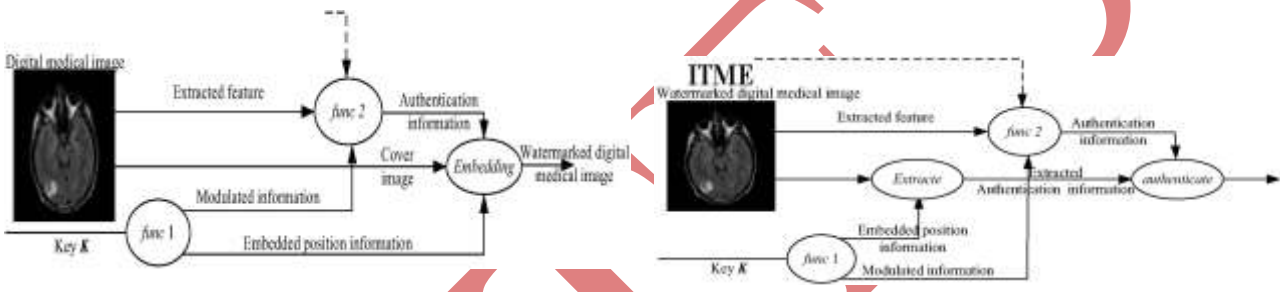
Figure 1 Non-Visible Watermarking

III. INTEGRITY AUTHENTICATION

Integrity authentication for digital medical images is important. When the doctor wants to diagnose the illness by using the digital medical images, we must make sure that the digital medical image is real, and they are not tampered. Meanwhile, if the digital medical images are tampered, we should not only know they are not integrated, but also can find the tampered area. Sometimes, the tamper images should have self recovery function. Here, we summary the watermarking technique for authenticating integrity from two parts: non-recovery authentication algorithm and self-recovery authentication algorithm.

3.1 Non-Recovery Authentication Algorithm

The basic procedure of non-recovery authentication Algorithm is as figure 2: the embedding diagram and



(a) (b)

Figure2 (A), (B) Basic Procedure Of Authentication Algorithm

In embedding diagram in figure 2(a), fuc 1 means that use key to generate the modulated information and embedded position information. The modulated Information is used to modulate the extracted feature form cover image for increasing the security. Sometimes, the Watermark image like the logo "ITME" is used in this Function. Then the authentication information is embedded into the Cover image according to the embedding position Information. When authenticate the reality or integrity of the using digital medical images, the authentication diagram in figure 2(b) is carried out. Firstly, the embedded authentication information is extracted, and then generates the authentication information like the generation in the embedding diagram. Compare the extracted authentication information and generated authentication information, and the different area is the tampered area. The important thing is these algorithms are the generation of attention information and the generation of embedding position information.

IV. DATA HIDING

In some special area, the digital medical images are so important that any change is not allowed. The distortion generated by watermark embedding will make the important information be lost, and it will lead dangerous. Meanwhile, the large amount of digital medical images will have much auxiliary information, such as the patients' name, gender, the information of illness, and so on. And the information will be lost or not match with corresponding digital medical image by mistake. Reversible data hiding scheme provides a good solution to this trouble. Since data hiding method allows people Embed information in a lossless manner that the digital host

image can be completely recovered after the data extraction. Reversible data hiding algorithms can be divided into three types, which are schemes based on Difference expansion, histogram shifting, and Prediction error expansion. Next, we will analyze these algorithms in detail.

4.1. Difference Expansion

The scheme of different expansion uses integer Transform to embed and extract data. The basic procedure of these algorithms is as follows:

Let (P0, P1) be the original pixel value in protected digital medical image, then the mean value and the Different are calculated:

$m = L (P0 + P1)/2.j , d = P1- P0$ (1)

Where, L • j denotes the floor operation which rounds the elements to the nearest integers towards minus infinity. Then binary data bit of watermark image W (WE (0, 1)) is embedded into the difference by expanding the different:

$d' =2xd+w$ (2)

Then the marked pixel value p0', p1' are calculated by

$P0'=m+L (d'+1)/2j, p1'=m-L (d)'/ 2j$ (3)

And (p0', p1') are the new pixel values III the

Watermarked image. The data extraction of difference expansion scheme is the inverse of data embedding, and the Procedure is as follows:

Firstly, the mean value is also calculated:

$m = L (p0'+ p1' / 2 j$ (4)

And the different value between the two pixels in Watermarked image is calculated:

$d'=p0-p1$ (5)

Then the embedded data is extracted by

$W = LSB (d')$ (6)

and the original different is recovery by

$d = L d'/2 j,$ (7)

Where the LSB represents the least significant bit extraction function. Finally, the original image is recovered as follows:

$P0 = m - L (d/2)J . PI1= m+ L (d +1) / 2$ (8)

Difference Expansion method is simple for integer transform, but the embedded amount is limited, and the highest embedded capacity is 0. 5bpp. For digital medical images, the texture is high, and the difference between the pixel pair is so large that the difference expansion makes

the pixel value overflow. Usually, we should use the location map to record the position of overflowed pixels, and the amount in this scene is less than 0. 5bpp.There are some other modified algorithms to improve the capacity.

For example, Alattar use pixel vector replace the pixel pair in Tian's method. And the capacity of these algorithms is as high as 2/3 bpp.

4.2. Histogram Shifting

Reversible data hiding schemes based on Histogram Shifting llluse the statistic character of host image to embed data. And the embedded amount is decided by two important elements named peak point and zero point Peak point is the pixel value with the most number, and zero point represents the pixel value with least number.

4.3 Embedding

The image is first divided into N_b non-overlapping image tiles (e.g. N_b =4, 16). The intensity histogram of each image tile is generated and, the following steps (2-4) are iteratively executed for each image tile. In each image tile, for a given number of n (peak, zero) pairs, the pairs are chosen such that the image quality is either maximized (least distances between the chosen pairs), or according to any other criteria such as perceptual quality.

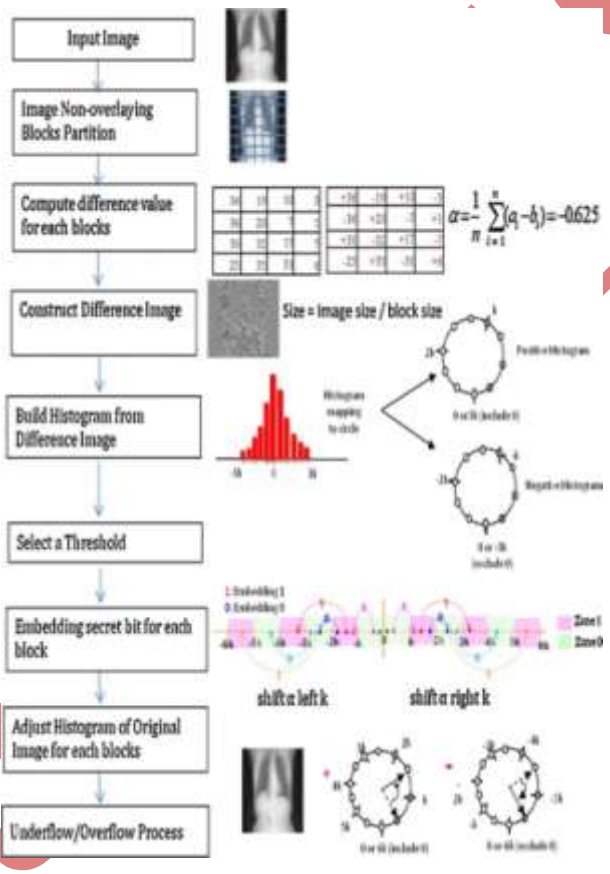


Figure 3: Flowchart Of Histogram Shifting

The (P_i, Z_i) pairs are then prioritized either based on objective or subjective quality, as explained above, with P_i and Z_i as the intensity of the peak and zero. The following iteration is executed n times for i =1: n. For pair (P_i, Z_i) the image tile is scanned and if: A) Pi > Z_i, the gray values of the pixels between Z_i+1 and P_i are reduced by one (shifting the range of the histogram [Z_i +1, P_i] by 1 to the left). This creates a gap at gray level P_i. The image tile is re-scanned and the gray values of the pixels with gray value of P_i -1 are incremented by one if the bits of the to be embedded data are "1", otherwise they will not be modified. B) Z_i > P_i, the gray values of the pixels between P_i +1 and Z_i -1 are increased by one. This creates a gap at gray value P_i +1. Then image tile is re-scanned and the gray values of the pixels with gray value of P_i are increased by one if the corresponding bits of

to be embedded data are "1", otherwise they will not be altered.

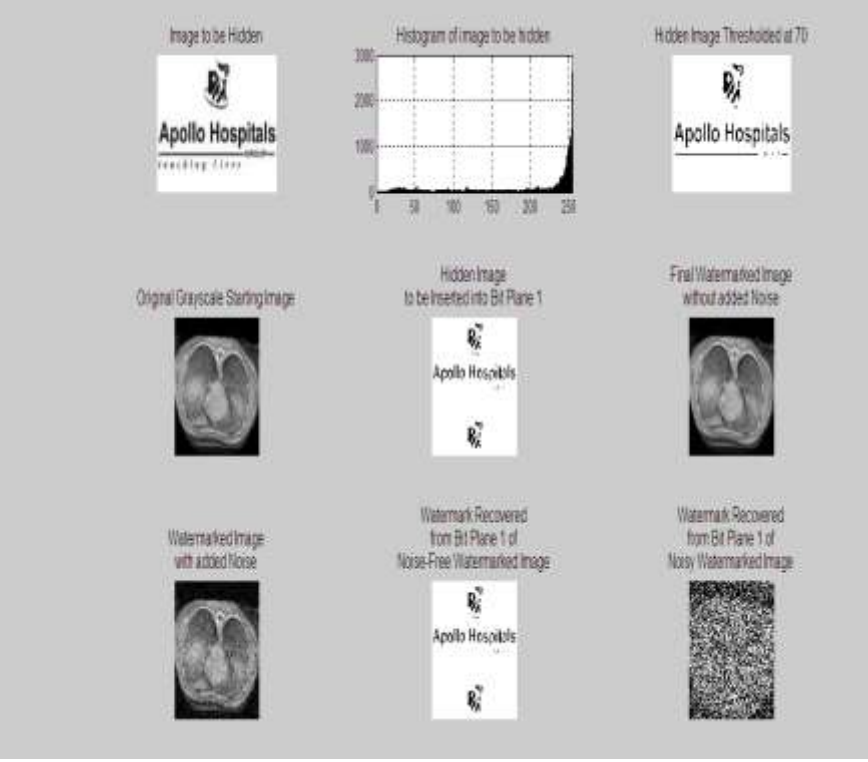
4.4 Detection

For the given N_b, their embedding order and n, the following process is used to extract the secret message from a marked image and the lossless recovery of the host image. Firstly, the image is divided into N_b image tiles. They are then rank ordered in their order of priority. Then steps 2-3 are repeatedly executed for each image tile. The following iteration is done n times for i =1: n. For pair (P_i, Z_i) the image tile is scanned and if:

1 $P_i > Z_i$, the pixel with gray value P_i indicates that the embedded data bit was 1 and it should not be modified. Otherwise, if it is equal to P_i-1, it indicates that the embedded data bit was 0. In this case, its gray value has to be increased by 1. Later on the gray values of all pixels with gray values between Z_i and P_i-2 need to be increased by one.

2 $Z_i > P_i$, the pixel with gray value P_i indicates that the embedded data bit was 0 and they do not need to be modified. However, if it is equal to P_i +1, it indicates the embedded data bit was 1. Then, its gray value is reduced by 1. Therefore, the gray values of all pixels with gray values between P_i +2 and Z_i are reduced.

V. RESULTS



5.1 Comparison Of PSNR Ratios:

Table 1.. Comparison of PSNR without adding Noise

	DWT	Difference expansion	Histogram shifting
PSNR	61.58%	10.009%	29.6006%

Table 2 Comparison of PSNR with adding noise

	DWT	Difference expansion	Histogram shifting
PSNR	36.008%	1.008%	10.666%

VI. CONCLUSION

This paper detail explains about the reversible watermarking technique of histogram shifting. The performance is calculated by PSNR value .the proposed method of histogram shifting having PSNR of 29**%.**

VII. FUTURE SCOPE

These techniques are applied to video for hiding data gives more results.

REFERENCES

[1] Digital image processing by GONALEZ 3rd Edition.

[2] L D Li, X P Yuan, Z L Lu, J S Pan. Rotation invariant watermark embedding based on scale-adapted characteristic regions. Information Sciences, 2010.180(15):2875 -2888

[3] J Tian. Reversible data embedding using a difference expansion. IEEE Trans on Circuits and Systems for Video Technology. 2003.13(8), 890-896.

[4] A.M Alattar. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image process. 2004.13(8).1147 -1156

[5] C C Lin, W L Tai, C C Chang. Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recognition. 2008.41(12):3582-3591

[6] D C Lou, C L Chou, H K Tso, C C Chiu. Active steganalysis for histogram-shifting based reversible data

hiding. Optics Communications, 285(10):2510-2518.

Biographical Notes

Ms. S. Mounika is presently pursuing M. Tech. final year in Electronics & Communication Engineering Department (Specialization in Systems & Signal Processing) from MRCET, Hyderabad, India.

Dr. M.L. Mittal is working as a Professor in Electronics & Communication Engineering Department from MRCET, Hyderabad, India.