International Journal of Image Processing and Vision Science

Volume 1 | Issue 3 Article 9

January 2013

A DYNAMIC WATERMARKING MODEL FOR MEDICAL IMAGE AUTHENTICATION

PRIYA. H. K
Dept. of ECE, EWIT, Bangalore, India, phk@gmail.com

ANITHA. S
Dept. of ECE, EWIT, Bangalore, India, a.s@gmail.com

A DYNAMIC WATERMARKING MODEL FOR MEDICAL IMAGE AUTHENTICATION

PRIYA. H. K[1] & ANITHA. S[2]

[1,2]Dept. of ECE, EWIT, Bangalore, India

Abstract – This paper proposes a dynamic watermarking model for the purpose of medical authentication. While transferring the data through a public network there is jittering or tampering of data. This is a matter of concern as any jitter or tampered data is not desirable in the medical field. It is noted that there is loss of life due to corrupted data received leading to wrong diagnosis. The proposed dynamic model proves that the medical image watermarked with the proposed system provides near lossless original image. Since the watermark is generated dynamically it is unique to the images considered therefore enhances the security of the images. The Proposed scheme is in the TIFF (Tagged Image File Format) using RGB colour space. The given watermark is embedded inside the image by expanding intraplane difference between any two colour planes of images.

Keywords - *Dynamic watermark, Integer Transform, Fundus Camera, Intra plane Expansion*

I. INTRODUCTION

Image processing is a fast developing field which can be used for the purpose of medical authentication. This research work presents a technique for the purpose of medical authentication. Authentication involves a challenge to determine whether the image and embedded data is received without any modification to the original image and embedded data

The embedded information watermarking techniques that embed information into a host image in a block-wise independent fashion is vulnerable to a vector quantization (VQ) counterfeiting attack [2-3]. Specifically, given a watermarked image, one can forge the watermark it contains into another image without knowing the secret key.

The digital fundus images are one particular class of medical images which has been chosen for simulation and analysis of the proposed scheme. These images are given in Tagged Image File (TIF) format in RGB colour. Correlation values are compared from different portions of the image, the technique enables us to distinguish malicious changes, such as replacing or adding features from no malicious changes resulting from common image processing operations space [1]

The proposed scheme dynamically generates the watermark using dynamic models. And, it is embedded inside the image by expanding intra plane difference between any two colour planes of images. It is known as intraplane difference expanding.

II. FRAMEWORK FOR DYNAMIC WATERMARKING SCHEME

The proposed scheme in this paper works in four stages.

- The first stage selects the reference color plane for generating watermark.
- The second stage uses the proposed dynamic model and generates the watermark using the reference color plane.
- The third stage involves embedding. This process is carried out using Integer transform.
- The fourth stage performs the extraction and verification process.

A. Selection of Reference Colour Plane

The green color is the selected reference plane to generate a watermark. A fundus camera is used which uses the special green filter for photograph of the fundus area. The image in the green channel contains all details along with other color plane.

B. Watermark Using Dynamic Model

The dynamic system is defined by the following equation,

$$x_{n+1}=f(x_n) \quad (1)$$

In this system the dynamic image changes with time. Though the behaviour is random it is deterministic.

These changes are very sensitive to the initial conditions. The sensitivity of the image increase exponentially to the growth of perturbations in the initial conditions. Therefore, the watermark is generated through dynamic system using the reference color plane as initial condition [1]. Thereby, the watermark is generated dynamically.

In the Proposed system, a hybrid optical bistable dynamic system is used which is defined by

$$f(x_n) = \sin^{(2)}(x_n - 2.5) \quad (2)$$

C. Embedding by Intra Plane Difference Expanding

The embedding process is carried out using integer transform by using Intra Plane Difference Expanding. In the Embedding stage, the original imaging (I,J,K) is divided into colour planes. Here I denote number of rows, J denotes number of columns

and K denotes number of planes. Since, the input image is in RGB (Red, Green, Blue) mode, k=3 in the proposed scheme. The green color plane will be used as seed to generate the watermark in messy system. Since, the watermark is generated dynamically; it will be unique to the images. Then, pixel pair is formed from the red and blue color planes of the images. By checking overflow and underflow condition for pixel pair, the watermark is embedded in the difference of the pixel pair by expanding the difference. This is known as intra-plane difference expanding.

The watermark is generated through dynamic system by using prominent pixel values of reference color plane of the image as seed. The initial values to the messy system is designed by

EffectiveKey (:,k1) = KeyIn((1+(k1-1)*M) : (((k1-1)*M)+M)); (3)

Where,(k1) refers the pixel values of reference color plane of the image. I refers embedding depth. The position information (pos) and secret key (key) is also used in the initial condition. The dynamic sequence is generated by substituting EffectiveKey (:,k1) value for Xn in Eqn.2.For the kth pixel the sequence is referred as EffectiveKey (:,k1), i=l, 2, 3 ...1. The reasonable number of iteration (I) is performed for the pixel to attain the dynamic status. This sequence contains floating numbers that is converted in to binary sequence in the proposed scheme. Hence, the thresholding T is introduced here to convert the sequence c_seq (k, i) from floating to binary sequence w (k, i). The w (k, i) is obtained by

$$W(k,i)=\begin{cases}1 & c\_seq(k,i) > T \\ 0 & elsewhere\end{cases} \quad (4)$$

Where, T is set to 8/3 by the number of test to bring equal number of zeros and ones. The length of sequence G is combined to one bit w (.) by applying XOR operation. Thus, the watermark is generated for the kth pixel. By repeating the same procedure for remaining pixels of the reference color plane of the image,the watermark is generated for the whole image for the Fig 1.

Fig.1 : Original Retina Image

Difference expansion transform is a remarkable breakthrough in reversible data-hiding schemes. The difference expansion method achieves high embedding capacity and keeps distortion low. The difference expansion method with the simplified location map and new expandability can achieve more embedding capacity while keeping the distortion at the same level as the original expansion method. This improvement can be possible by exploiting the quasi-Laplace distribution of the difference values.

Integer Transform: For a 8 bit gray scale pixel pair (x, y), 0::; x, y ::; 255, the integer transform is given by the pair (m, d).Where m refers integer average and d refers difference

$$M=\left\lfloor\frac{x+y}{2}\right\rfloor \quad (5)$$

$$d = x-y \quad (6)$$

The inverse transform is given by

$$x = m + \left\lfloor\frac{d+1}{2}\right\rfloor \quad (7)$$

$$y=m-\left\lfloor\frac{d}{2}\right\rfloor \quad (8)$$

Where L, J refers floor operation which rounds the value to nearest integer, in the integer transform, the difference (d) is modified based on the watermark bit (bit) to hide the bit into the pixel pair. The modification of difference (d ') is given by

$$d' = 2 * d + bit \quad (9)$$

The modification process checks two conditions. They are overflow and underflow. It is done to ensure that the difference is expandable or not. The expandable difference should satisfy the following condition.

$$|d| \le 2 * (255 - m) \;\; if\; 128 \le m \le 255$$
$$|d| \le 2 * m + 1 \;\; if\; 0 \le m \le 127 \quad (10)$$

Only expandable difference can be used for embedding. If all the expandable differences are used, the capacity will reach its limit. Let N and Ne denote the number of differences and the number of expandable differences, respectively. The hiding capacity of an image is defined as:

$$c=\frac{Ne}{N} \quad (11)$$

D. Extraction and Verification

In the extraction process, the watermarked image is processed in the same way as original image processed for embedding. The extraction process is complete blind. Both original image and original watermarks are not used for the extraction process. Extraction process produces the reference sequence using messy system and green color plane as seed. The embedded watermark is extracted by applying inverse integer transform using Eqn. 6 and Eqn.7. Where, the LSB (Least Significant Bit) of the difference value gives the embedded watermark bit.

The reference sequence and the extracted watermark sequence are compared to check that whether the given volume of the image is tampered or not. The difference between reference sequence and

the extracted watermark sequence will show the tampered volumes in the image as shown in fig.3. Thus, the extraction process works in complete blind way and enhances the security. The extraction process in this paper is reversible. It means that the original image should be retrieved without any loss after removing the watermark at the extraction stage. The medical images were exchanged from one place to another for diagnosis purposes. Hence, the loss in the quality of images is not accepted here.

Results and Snapshots

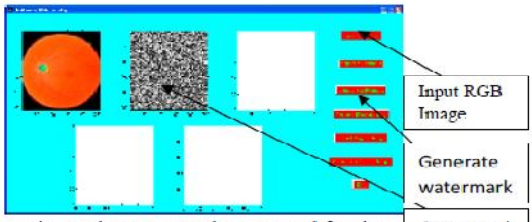

Fig. 2 The watermark generated for the whole image

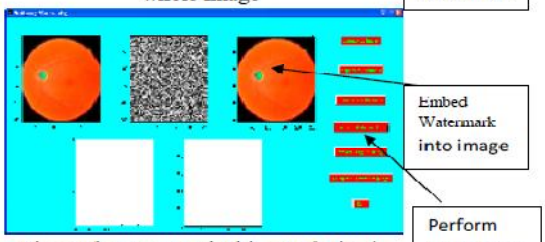

Fig. 3 The watermarked image (Wimg) generated for the given original image (Img).

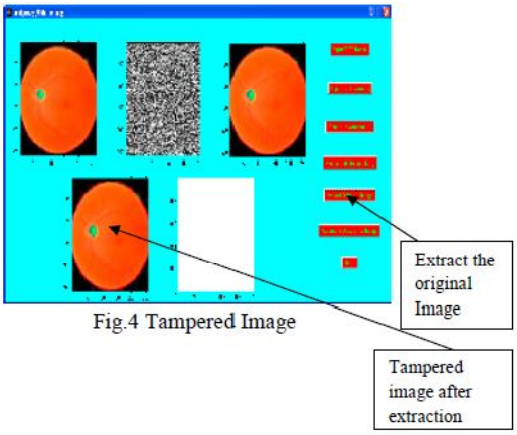

Fig.4 Tampered Image

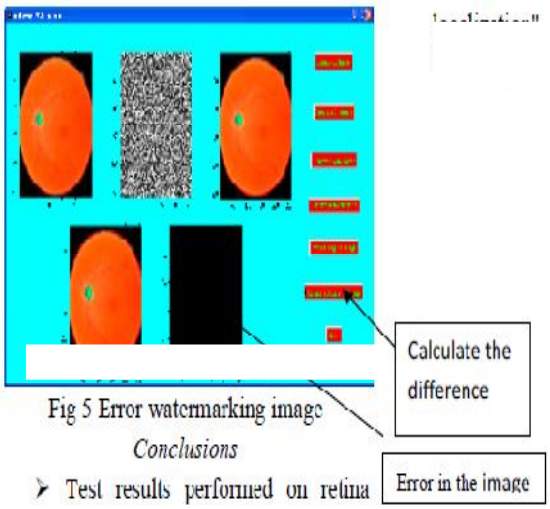

Fig 5 Error watermarking image

Conclusions

- Test results performed on retina

III. CONCLUSIONS

- Test results performed on retina image i.e. JPEG format, RGB color mode confirms that we can authenticate whether the received image is with or without any modification.
- Enhances the security of medical image.
- By the test results we can conclude that "A Dynamic watermarking Model for Medical Image Authentication" can be used to detect authenticity of received image precisely.

REFERENCES

[1] S.Poonkuntran, R.S.Rajesh," A Messy Watermarking for Medical Image Authentication", IEEE 2011

[2] M.Wu, B. Liu,"Watermarking for image authentication", in:Proceedings of the IEEE International Conference on Image Processing, Chicago, IIIinoise,US, (1998), pp. 437-441.

[3] M. Holliman, N. Memon, "Counterfeiting attacks on oblivious blockwise independent invisible watermarking schemes", IEEE Trans. Image Process. 9 (2000) 432-441.

[4] M.U. Celik, G. Sharma, E. Saber, AM. Tekalp,"Hierarchical watermarking for secure image authentication with localization", IEEE Trans. Image Process. 11 (2002) 585-595.

◈◈◈