International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Authenticated Medical Image Transmission using Enhanced Reversible Data Hiding (RDH) with NNP^2 Algorithm and Rhombus Prediction

R Gomathi

Abstract: ***During the last few years, the medical information of concerned patient is transferred from one doctor to another doctor via internet for better diagnosis and studies. Transferring medical information over a transmission medium is known as telemedicine. Telemedicine has been used to overcome distance barriers and to improve access to medical service. The telemedicine application includes emergency treatment, home monitor, military applications, and medical education. These medical images are corrupted by hackers when it is transferred through internet. Hence security of medical images is necessary. Watermarking is used for providing security while transferring medical images. Reversible Data Hiding (RDH) is one of the efficient methods for secure transmission of medical images. In this method, data hiding capacity is very small and the distortion level of recovers images is very large. To avoid these drawbacks, Nearest Neighborhood Pixel Prediction (NNP^2) algorithm based on Chinese Remainder Theorem (CRT) is proposed and Rhombus Prediction is applied in NNP^2 to increase data hiding capacity. The distortion level is reduced by Histogram Shifting. The performance of proposed method is evaluated using PSNR for number of medical images. The results shows that the proposed method gives good results when compared with traditional methods.***

Keywords ***: Watermarking, Telemedicine, Reversible Data Hiding, Medical image.***

I. INTRODUCTION

During the most recent couple of years, the therapeutic data (patients report) is moved starting with one specialist then onto the next specialist by means of web for better finding and contextual investigations [1], [2]. Moving therapeutic data over a transmission medium is known as ***telemedicine [3], [4]***. ***Telemedicine is the utilization of therapeutic data traded starting with one site then onto the next by means of electronic correspondences to improve a patient's clinical wellbeing status and administrations utilizing two-way video, email, PDAs, remote apparatuses and different types of broadcast communications innovation.*** Telemedicine has been utilized to defeat distance barriers and to improve access to restorative administrations.

The telemedicine application incorporates crisis treatment, home screen, military applications and therapeutic instruction [5], [6]. At the point when a restorative picture is defiled or altered by somebody during its transmission over any open access arrange, it prompts deviations in the analysis which may make genuine medical problems for any person. In this manner, the security of restorative picture is important. These restorative pictures are tainted or the substance of the picture is altered by programmers when it is moved through the web and through another transmission medium. Different approaches and systems are accessible for the security of restorative picture [7],[8].

The computerized watermarking method is one of the answers for the security of therapeutic pictures. The installed watermark ought not influence the nature of the first picture. Reversible Data Hiding (RDH) is one of the productive advanced watermarking strategies for verified transmission of medical images. But, in this method, the data hiding capacity is very small and the distortion level of recovered images is very large.

To avoid all these drawbacks, a Nearest Neighborhood Pixel Prediction (NNP^2) algorithm which is based on Chinese Remainder Theorem (CRT) is proposed and Rhombus Prediction will be applied in NNP^2 to increase the data hiding capacity. The distortion levels will be reduced by using Histogram shifting.

II. PROPOSED METHODOLOGY

A. Reversible Data Hiding

Reversible Data Hiding is a procedure for installing data into spreads, for example, picture, sound and video documents. RDH or lossless information stowing away is a strategy by which unique spread can be losslessly reestablished after inserted message is removed. Reversible Data Hiding comprises of Nearest Neighborhood Pixel Prediction (NNP^2) algorithm and Rhombus Prediction which uses Chinese Remainder Theorem (CRT). The Frame work of the proposed methodology is shown in Figure 1.

B. Nearest Neighbourhood Pixel Prediction (NNP^2)

The test input is an X-ray of a Lungs image.

Manuscript published on November 30, 2019.
* Correspondence Author
R Gomathi*, Department of ECE, University College of Engineering Dindigul Campus, Dindigul, Tamilnadu. Email: gomathiaudece@gmail.com

The image of the concerned patients face will be considered as the watermark. Prediction Error Expansion (PEE) scheme can embed only 2 bits in an expandable pixel, whereas in the proposed NNP[2] algorithm, it can embed 6 bits almost into one expandable pixel. The secret message to be transmitted will be embedded using this algorithm.

C. Chinese Remainder Theorem (CRT)

CRT provides a solution for congruence system

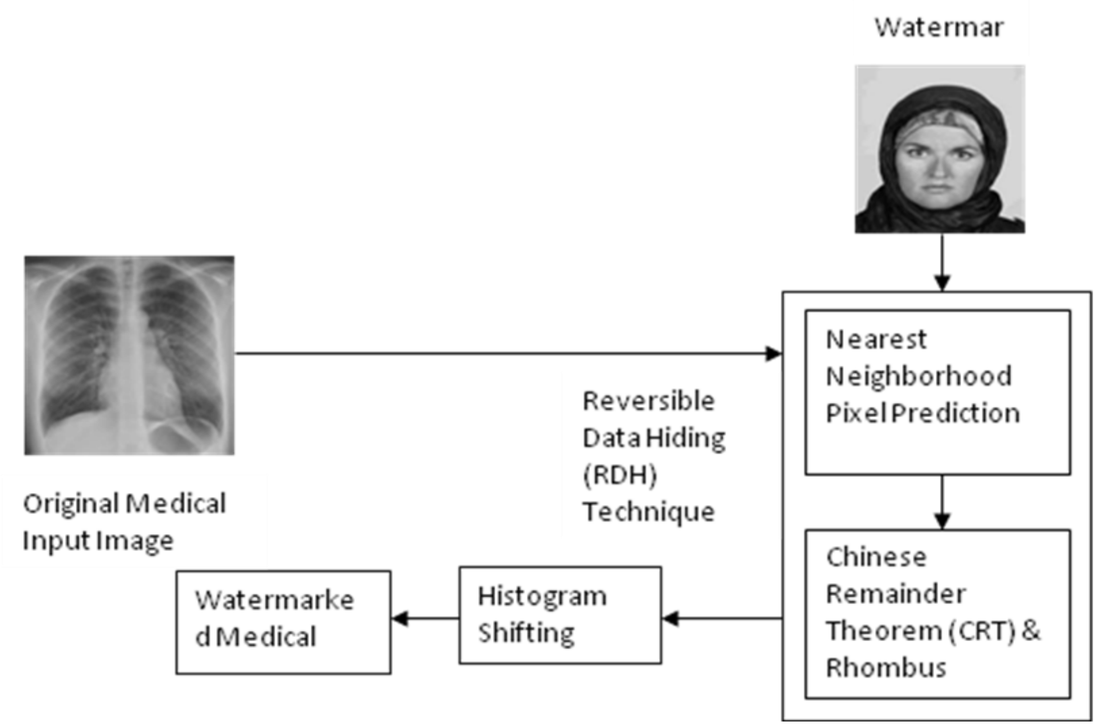

Figure 1 Framework of Proposed Methodology

$$C = \left(\sum_{i=1}^{m} x_i * N_i * a_i \right) \bmod N$$

where, (1)

$$N = n_1 \times n_2 \times \ldots\ldots\ldots\ldots \times n_m = \prod n_i$$

$$N_i = N / n_i$$

$$a_i = N_i^{-1} \bmod N$$

D. Rhombus prediction

The Pixels of the image are divided into 2 categories, white dots and black dots. Figure 2 shows the four black pixels adjacent to white pixels form a rhombus pattern.

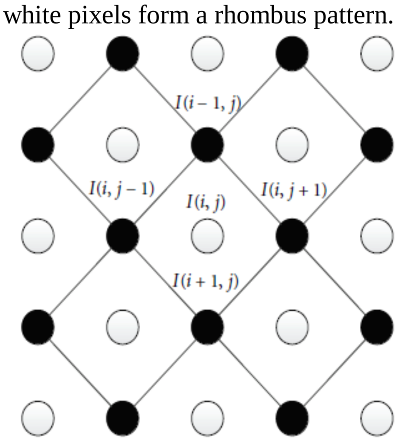

Figure 2 Rhombus prediction scheme

The white pixel value is predicted by 4 neighboring black pixels and vice versa. The four black pixels are located in four corners of the rhombus; white pixel is located in center of the rhombus. So, the corresponding prediction value $p_{i,j}$ is given by,

$$p_{i,j} = \frac{\lfloor TI_{i,j-1} + TI_{i-1,j} + TI_{i,j+1} + TI_{i+1,j} \rfloor}{4}$$

The calculated value of C will be embedded into the original value of pixels. The watermarked pixel value is given by,

If $0 \le D < p$

$$w_{i,j} = \begin{cases} p_{i,j} + C, & TI_{i,j} \ge p_{i,j} \\ p_{i,j} - C, & TI_{i,j} < p_{i,j} \end{cases} \quad (2)$$

If $D \ge p$

$$w_{i,j} = \begin{cases} p_{i,j} + T, & TI_{i,j} \ge p_{i,j} \\ p_{i,j} - T, & TI_{i,j} < p_{i,j} \end{cases} \quad (3)$$

Where,

$w_{i,j}$ is the watermarked pixel value of $TI_{i,j}$

T is the threshold.

By this embedding algorithm, the prediction value of white pixel is calculated from the neighboring black pixels and vice versa. The receiver can extract the hidden watermark image by using the same scanning method as used during the embedding algorithm.

Retrieval Number: D8847118419/2019©BEIESP
DOI:10.35940/ijrte.D8847.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The original pixel value is calculated using the equation,

$$TI_{i,j} = \begin{cases} p_{i,j} - C, & w_{i,j} \geq x \\ p_{i,j} - T, & elsewhere \end{cases} \quad (4)$$

where,

$$T = p \times (q-1) \text{ (Threshold)}$$

E. Histogram Shifting

The output watermarked image of RDH technique will be subjected with Histogram Shifting to reduce the degree of Distortion level. The histogram is a graph showing the number of pixels in image at each different intensity value. Pixels with value [0, L-1] are shifted to [L, 2L-1]. Overflow and underflow problems may occur, when watermarked pixel is out of range of (0, 255) in the watermarked image. Histogram shifting will be required to solve these under flow and overflow problems also. ***The output watermarked image of Histogram Shifting will be better than the existing methods in terms of imperceptibility, robustness, and security.***

III. RESULTS AND DISCUSSIONS

For testing, the various medical images are acquired and subjected to the proposed algorithm. The size of the input sample images are 256×256. For example, the acquired medical image is shown in Figure 3.

Figure 3 Sample test input

A. Rhombus Prediction and Watermarked image

In order to find the prediction value of center white pixel, the four adjacent neighbouring black pixels in the shape of rhombus is considered, hence named Rhombus Prediction. The prediction value of white pixels is calculated from neighbouring black pixels. So, while embedding watermark into the white pixels, the value of black pixels remains unaltered. The calculation of prediction value is shown in Figure 4.

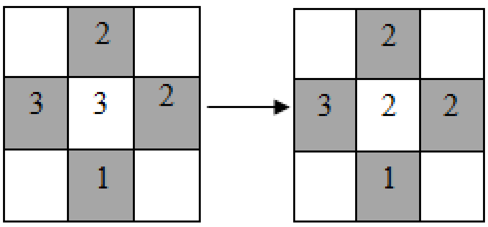

Figure 4 Calculation of prediction value

The difference between the original and predicted value of pixels is the absolute value and is calculated from the Equation,

$$D = \left| I_{i,j} - p_{i,j} \right|$$

Where,

$I_{i,j}$ is a value of original pixels

D is a difference between original and predicted value of pixels.

To calculate the integer C using CRT, read N bits from the watermark. The N bits are calculated using the Equation $N = \log(q)$. For a congruence system, $\{n_1, n_2\} = \{3,5\}$ co prime numbers, whose GCD value is 1. The value of C is obtained using the Equation (1).

Case 1: on embedding binary information (000001)

Table 1 Decimal values of binary watermark

Binary Information	0	1
(x) Decimal value	0	1

As atmost 6 bits can be embedded into one expandable pixel, binary information to be embedded is splitted into two parts, each with three bits and decimal values of the corresponding binary information is shown in Table 1.

Case 2: on embedding a character ('A')

The character 'A' is converted into binary information, the ASCII value contains 7 bits. The binary information is splitted into two parts, each with five bits, further five bits are splitted into three bits and two bits. The corresponding decimal value is shown in Table 2.

Table 2 Decimal values of character watermark

Embedding character 'A'				
Binary value of A	000	10	000	01
Decimal value (x)	0	2	0	1

The calculated decimal values are applied in the Equation (1) to calculate the integer C. The value of C is superimposed on the predicted white pixels and the black pixels remains unchanged. Thus the watermark is embedded into the original input sample medical image.

The watermarked image is obtained by superimposing original input sample medical image with watermark. The watermark may be either the binary information or text information. The watermarked pixel values are obtained from Equations (2) & (3) respectively. The watermarked image is shown in Figure 5.

Retrieval Number: D8847118419/2019©BEIESP
DOI:10.35940/ijrte.D8847.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Figure 5 Watermarked image

B. Extraction of Original Image

In the extraction process, at the receiver side, after receiving the watermarked image, the receiver can extract the hidden message and the original input sample image from the watermarked pixel without any distortion. The difference between the watermarked pixel and prediction value is calculated and the hidden message can be extracted using $x = C' \bmod N$. The extracted decimal value x of the watermark is given as,

Case 1: on embedding the binary information (000001)

Table 3 Extraction of hidden information

x Extracted decimal value of	0	1
Binary value of x	0	1

If the binary information (000001) is considered as watermark, after embedding the binary information, the extracted decimal and binary value of x is given in table 3.

Case 2: on embedding the character (‘A’)

If the character (‘A’) is considered as watermark, the extraction of the character is shown in Table 4.

Table 4 Extraction of hidden character

decimal value of x	0	2	0	1
Binary value of x	000	010	000	001
Extracted Character ‘A’				

The original input sample image can be losslessly recovered from the watermarked image while embedding the binary information using the Equation (3), the extracted original image is shown in Figure. The output image is subjected with histogram shifting to reduce the distortion level. To prevent the overflow and underflow, the histogram is shifted. The histogram of extracted image is shifted to $L = p \times q - p$ units. Based on the above condition, while p and q, are both integers, the value of q is set as multiples of 2, 4,8,16,32 or 64 which means one pixel can embed 6 bits atmost. The image of the original image after histogram shifting is shown in Figure 6.

Figure 6 Image after histogram shifting

C. Experimental Evaluation

PSNR in decibels is computed between the two images. The ratio is often used as a quality measurement between the original and the extracted image. The higher the value of PSNR, better the quality of the reconstructed or the extracted image.

The MSE and the PSNR are the two error metrics used to compare the image quality. The comparison of PSNR values between the existing and the proposed methods are shown in Table 5. Table 5 shows the range of PSNR values for the existing and proposed methods for different input sample images. It is observed that PSNR values of different input sample images for the proposed method shows better and higher results when compared to the already existing methodologies. The higher values of PSNR shows the better quality of reconstructed or the extracted images.

Table 5 Calculation of PSNR

Sample images	PSNR (dB)	
	Existing Method	Proposed Method
Test input 1	48.42	61.33
Test input 2	58.01	62.56
Test input 3	46.37	70.11
Test input 4	46.47	65.38
Test input 5	55.5	64.17

IV. CONCLUSION

In this paper, secured medical image transmission is proposed using image processing techniques. Medical images are taken as original images. Watermark is embedded into original image to be transmitted by using NNP^2 algorithm. Initially, the binary information is used as watermark. During the extraction, binary information is perfectly extracted and the original image is losslessly reovered without any distortion. The performance of the proposed method is evaluated using the performance measures PSNR for number of medical images. The results show that the proposed method gives good results when compared with the traditional methods. Hence, this method is used in real time applications like telemedicine. Then, a character, for example ‘A’ is used as a watermark. In this, while recovering the original image, character is extracted but the original image is subjected with small amount of distortion.

In future, this work will be extended to avoid the distortion that occurs in original medical images while embedding the character as watermark.

REFERENCES

1. G Amina Saleem, Karim Abed Meraim, (2009) 'Watermark extraction using blind image separation and sparse representation', International journal of engineering and computer science.
2. Ashwinin Gakar, R. Rokade, S.M. (2016) 'Data hiding with contrast enhancement by using RDH algorithm', International journal of engineering development and research, Vol. 4, pp. 2321-9939.
3. Jasni Zain, M. Abdul Fauzi, R.M, (2010) 'Medical image watermarking with tamper detection and recovery', International journal of engineering and computer science.
4. Namita Tiwari, abha singh sardar. (2017) 'Advancement in reversible data hiding techniques', International journal of computer science and network security, Vol. 17, No. 3.
5. Hee joon Hwang, SungHwan Kim, Hyoung Joong Kim, (2016) 'Reversible data hiding using least square predictor via the lasoo', EURASIP journal on image and video processing.
6. Shilpa shreekumar, Vincy salam, (2014) 'Advanced reversible data hiding with encrypted data', International journal of engineering trends and technology, Vol. 13, No. 7.
7. Babu, M V S S. Suseela, D V L. Prasanna lakshmi, Jyothi, A. (2017) 'A Novel approach for diital image watermarking', International journal of ECE, Special issue.
8. Sukhdeep Kaur, Manshi Shukla, (2014) 'Reversible data hiding and its method', International journal of computer science and mobile computing, Vol. 3, pp. 821-826.

AUTHORS PROFILE

R Gomathi is currently working as Assistant Professor at University College of Engineering Dindigul Campus, Dindigul, Tamilnadu. Her special fields of interest included Digital Image Processing, Remote Sensing and Neural Networks and Applications.