ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

Reversible Watermarking Techniques In Image Authentication Using LSB Data Hiding

S.Kumaravel [1], vaidyanathani[2], P.Vinayagam[3]

Associate Professor, Department of Electronics and Communicaton Engineering, SKP Engineering College

Tiruvannamalai, Tamilnadu, India [2]

Assistant Professor, Department of Electronics and Communicaton Engineering, SKP Engineering College

Tiruvannamalai, Tamilnadu, India[1, 3]

ABSTRACT: With the recent growth of networked multimedia systems, techniques are needed to prevent (or at least deter) the illegal copying, forgery and distribution of digital audio, images and video. An efficient digital watermarking scheme to transmit the medical image which embeds an encrypted data is proposed in this paper. A generalization of the well-known least significant bit (LSB) modification is proposed as the data-embedding method. We substitute the non-significant LSB bit plane of the medical image with encrypted data with authentication code. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion and transmitting these compressed descriptions as a part of the embedded payload.

On the receiving side, the data contained in the LSB bit plane is decrypted using the authentication code. The resulting scheme enables on a side the exact recovery of the original image that can be unambiguously authenticated, and on the other side, the patient information to be saved or transmitted in a confidential way. We conclude that watermarking has found a niche role in healthcare systems, as an instrument for protection of medical information, for secure sharing and handling of medical images. The concern of medical experts on the preservation of documents diagnostic integrity remains paramount

KEYWORDS: Watermarking,PSNR, LSB,Encryption,Decryption.

1. INTRODUCTION

In recent years, with the development of the Internet and multimedia technology, It is more easy to produce, distribute, acquire and copy digital media products such as digital text, image, video and audio [1]. That is why, it is necessary to protect the digital production. The digital watermark technique can solve the problem. The digital watermark represents the ownership of the owner according to the embedding information into the original image. It can be applied to different applications including digital signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control, and secret communication [2]. Usually, an effective digital watermark scheme provides the three major properties [3]: (i) Imperceptibility (ii) Robustness and (iii) Unambiguity. The watermark which is embedded must be imperceptibility and invisible because of two primary concerns; firstly we should not lower the quality of the original image or it will break the aesthetic feeling and diminish the commercial value of the original**.** Second, if the watermark embedded is detected by hacker, it will be easily broke or be removed. So the watermarked image should be robust against attacks. The watermark could still be extracted clearly after some digital image processing such as noise, copy, deleting, scaling, lossy or lossless image compression ect. In the watermark extraction process, it should be unambiguous to prove the ownership of the owner [3]. One of the primary watermarking designing considerations is that the invisibility and robustness often collide [4]. In order to improve the robustness of the watermarking scheme, we embed multiple watermark copies to enhance the robustness of the proposed algorithm. It seems like that the original image has been interfered with much more noise. On the other hand, in order to keep the quality of the original image, we embed less information and high robust of the watermarking scheme. Usually, there are two kinds of basic watermarking design scheme [4][5]: Spatial domain and Transform domain or frequency domain (DCT, DWT, DFT). The watermark is more robust in the frequency domain than in the spatial domain. So the method embed watermark in frequency domain.

There are many researches on grayscale images have been done but robust watermarking scheme for color images is not sufficient. Now color images are dominant most of the parts of applications. Embedding information in color image RGB color channel is highly correlated so it is not suitable for embedding watermark. Some proposed embedding schemes focus on embedding watermarks in the Y component (luminance) in YIQ model. Kutter et al [6] embed the watermark by modifying selected set pixels in the blue channel because of its low sensitivity to human perception. The blue channel is the best choose to JPEG compression among the RGB because of its low sensitivity to human perception. So the hidden watermark is easy to be lost. Main problem of algorithms embedding watermark into red Channel is its very large energy loss. When the RGB true color image is compressed into JEPG, the embedding watermark in the red channel is easy to lost and difficult to extract. Otherwise green channel can endure JEPG compression and the embedded watermark is robust. So our select is Green channel to embed watermark information.

In this paper, a new robust DWT based color image digital watermark embedding and detection algorithm is proposed which embeds a meaningful random real number sequence into low frequency of G component sub-band. The rest of the paper is organized as follows. Section 2 is DWT and Watermark Model Analysis, Section 3 presented Watermark embedding and detection algorithm in detail. Section 4 Described experiments result,and finally section 5the conclusions.

II. DWT AND WATERMARK MODEL ANALYSIS

The DWT is a hierarchical sub-band system, where the sub bands are logarithmically spread in frequency. The green channel of the color image is extracted and decomposed by three levels DWT and we get the results GLL3 GLH3, GHL3, GHH3 .GLH2, GHL2, GHH2 and GLH1, GHH1, GHL1. The sub-band levels GLH1, GHH1, GHL1 and GLH2, GHL2, GHH2 are the high frequency of the green channel. So if we embed watermark message into such a high component channel, watermark will be too fragile to sustain even slightly image attacks and possibly be removed easily. Embedded watermark information and considered its results of Lena test image in each level of DWT resolutions (levels 1, 2 and 3), we get the PSNR are 40.06 dB, 45.27 dB and 50.01 dB [7]. The degradation of watermarked image embedded in level three is better than the other levels. In the level three GLH3 and GHL3, coefficient values are very small, the visual quality of the host image will be degraded. So it decreases the robustness of the watermark. For this reasons we select the low component channel GLL3 to embed watermark information. The embedded watermark information can be distributed to the whole image after the watermarked image is reconstructed. So the embedded watermark is robust against attack.

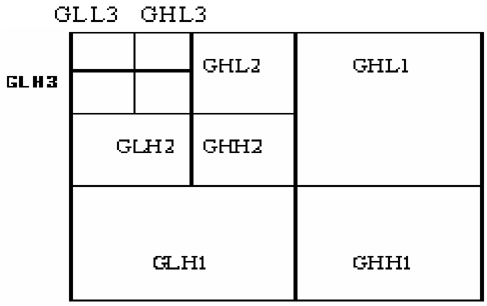


Figure.1 DWT three level decomposition flow chat of a color image

The original image cover data C_0 as noise like signals and add watermark w to the cover C_0 [8] , can be expressed as array C_w by

$$C_w = C_0 + w \qquad (1)$$

III. THE PROPOSED ALGORITHM

A. WATERMARK EMBEDDING

The watermark message is a random real number of a sequence of bits embedding into low frequency of G component sub-band GLL3. In our watermark embedding process the watermark is, W=W1,W2,W3,…,Wn. The process of embedding starts with the following steps:

Step 1 We first use key key1 to generate a random numbers sequence P=P1,P2, P3,…,Pn. Then determine a threshold T. So we can use Eq.(2) to define the watermark sequence.

$$W(k)=\begin{cases}1, & if \quad P(k)\geq T\\ \text{-}1, & elseif \quad P(k)<T\end{cases} \qquad \text{..............................(2)}$$

Step 2 Suppose the host color image size I = M×N. Use G component of RGB color image as carrier of embedding watermarking, then get GLL3 passing through 3 levels DWT into G component.

Step3 Use a key2 to determine starting embedding location of GLL3.

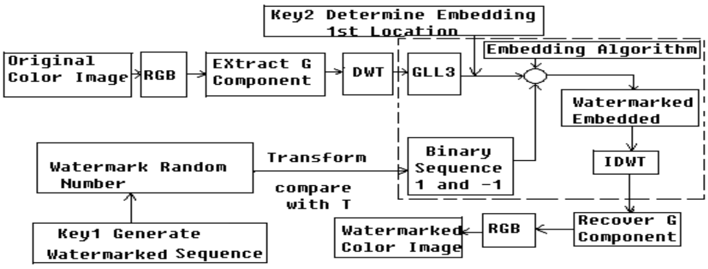


Figure.2 Watermark Embedding Algorithm flowchart

Step 4 The hidden watermark strength is determined by the ratio of the coefficient square values to the mean of sub-band $GLL_{3.}$ The larger the ratio is the larger strength of the hidden watermark can be chosen. The mean energy of the sub-band GLL3 , denote by E ; computed as follows:

$$E=\frac{1}{N^2}\sum_{x=1}^{N}\sum_{y=1}^{N}C^2(x,y) \qquad (3)$$

C(x, y) is the coefficient and denote the pixel value at the position (x,y) in the sub-band GLL3. N is the total number of wavelet sub-band GLL3. We Convert two dimension of C²(x,y) into one dimension sequence than resorted by C′(k)=GLL3′ (k), K = 1,…, MN/64. The length n of sequence $GLL_3\ (k)$ is selected to embed watermark. The watermark strength α is determined by

$$\alpha=\begin{cases}\alpha_1, if & 3\leq GLL_3^{'2}(k)/E\\ \alpha_2, if & 2\leq GLL_3^{'2}(k)/E<3\\ \alpha_3, if & 1.5\leq GLL_3^{'2}(k)/E<2\\ \alpha_4, if & GLL_3^{'2}(k)/E<1.5\end{cases} \qquad (4)$$

Step 5 Define following rule to embed watermarking

$$GLL_{3w}^{'}(k) \ = \ GLL_3^{'}(k)+\alpha\times W(k)\times|GLL_3(k)| \qquad (5)$$

$GLL_3^{'}(k)$ is the watermarked low frequency coefficient, k = 1,2,…,n. α is threshold to control invisible degree and robustness, where α>0. Finally, One dimension convert into two dimension after that IDWT is applied to GLL3 resulting is watermarked G component. Then we get watermark color image.

B. WATERMARK EXTRACTION

Step 1 Suppose, the green component of the host image denoted by Ig and watermarked image denoted by Ig*. Transform the image Ig and Ig* from RGB color space and get the G and G* component.

Step 2 The G and G*component are decomposed by three-level DWT to get the low sub-bands GLL3 and GLL3*. The coefficients GLL3 and GLL3 resorted by size, denoted GLL3(k) and GLL3*(k).

Step 3. The coefficient are compared is given by.

$$W(k)=\begin{cases}1, & if \quad GLL_3^*(k)\geq GLL_3(k)\\ -1, & elseif \quad GLL_3^*(k)\leq GLL_3(k)\end{cases} \qquad (6)$$

Step 4 The watermark is extracted from the watermarked image by the inverse transform of the watermarking embedding process (see Figure 3) During the transmission and distribution process the watermarked message maybe modified so the recover watermark is different from the original one. Set a constant threshold T to determine the sequence bit is 1 or -1.

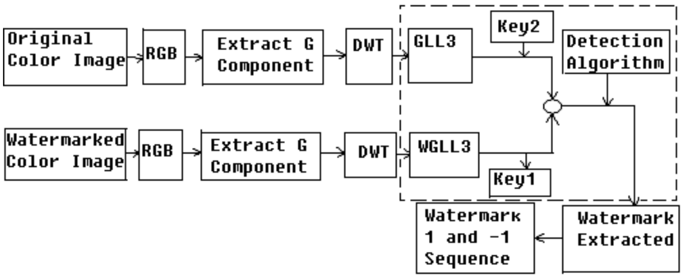


Figure.3 Watermark Extraction Algorithm flowchart.

Step 5 After extracting the watermark, we can compare extracted outcome with the original watermark. Therefore, a similarity measurement of the extracted and the referenced watermarks can be defined by the normalized correlation (Nc) [9]

$$Nc=\frac{\sum_{x=1}^{n}\sum_{y=1}^{n}W(x,y)\times\sum_{x=1}^{n}\sum_{y=1}^{n}W^{'}(x,y)}{\sum_{x=1}^{n}\sum_{y=1}^{n}W(x,y)^2} \qquad (7)$$

Finally the extracted watermark bit is recovered into a sequence.

The watermarking is a process of embedding an image or data into an image with which the cover image can be transferred or transmitted safely to the other end user. The coding or embedding process is involved in this project. In the result, the cover image and data is embedded using a password authentication. During recovery the cover image is separated from the data for further use

When the output is executed the GUI is shown initially as output. In this page a cover image has to be selected. The cover image is selected using the browse option.

Then the file name of the watermark image is document is selected .before starting the watermarking process a password is required for authentication. The four digit password is given and watermarking process is started.

The original image and the watermarked image is shown in this screen.

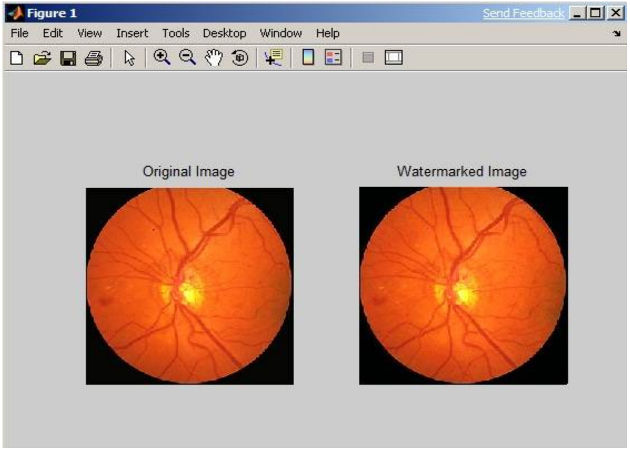
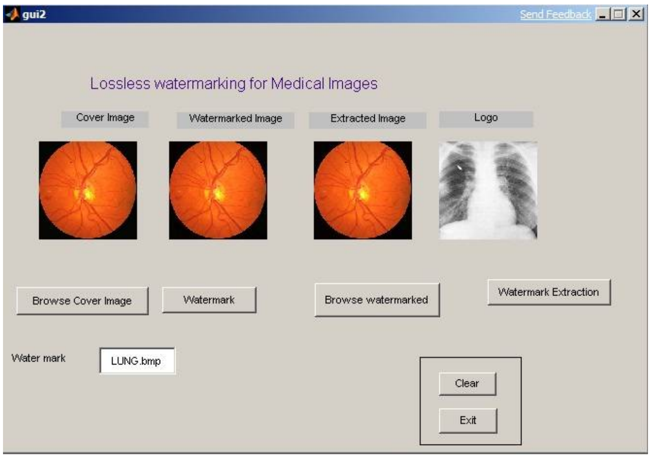


Fig: 1Original & Watermarked Image

When the watermarked content is selected for extraction the password authentication is required



Water mark: LUNG.bmp

Fig: 2 Final Output

V.CONCLUSION AND FUTURE WORK

A. CONCLUSION:

Watermarking technique present a new lossless image authentication framework, this offers computational efficiency, public/private key support and improved tamper-localization accuracy. Wireless communication technology has provided increased opportunity for applications such as military purpose, telemedicine targeting the communication of digital diagnostic images to remote locations for diagnosis and treatment.

The system was verified with valid as well as invalid data in each manner. The system is done with an insight into the necessary modification that may require in future. The proposed framework is flexible and compatible with the existing lossless (reversible) data embedding and fragile image authentication algorithms.

We have demonstrated a specific implementation of the framework using hierarchical image authentication and lossless G-LSB data embedding method. The framework can also be easily implemented using other fragile authentication and lossless data embedding method.

B. FUTURE WORK

The next goal is to implement this technique for the audio and video files as host image and also as the payload information. This can also be done for ROI segmentation by separating the foreground information from the background information and hiding the foreground information inside the background so that if there is any change in the foreground information it can be reconstructed from the background information. This can also be done for many clients using the public-private key algorithm in cryptography.

The watermarking algorithms can be improved and a better algorithm can be designed with which the data integrity, security, authentication can be improved and the process of watermarking can be efficient and speedy.

The data embedding technique used in this project is LSB insertion which is the famous method widely used. The other techniques has its own advantages and disadvantages and these methods can be used to improve the performance of the data embedding

REFERENCES

1.Celik M.U., Sharma G, Saber E, and Tekalp A.M (Oct 2001) - "A hierarchical image authentication watermark with improved localization and security," in Proc. IEEE ICIP, Thessaloniki, Greece, pp. 502–505.
2.Celik M.U., Sharma G, Tekalp A.M., and Saber E (Jan 2003), "Localized lossless authentication watermark (LAW)," Proc. SPIE, Vol. 5020, No. 1.

3.DeVleeschouwer C., Delaigle J.F., and Macq B (Mar 2003), “Circular interpretation of bijective transformations in lossless watermarking for media asset management,” IEEE Trans. Multimedia, Vol. 5, No. 1, pp. 97–105.
4.Hartung F and Kutter M (Jul 1999), “Multimedia watermarking techniques,” Proc. IEEE, Vol. 87, No. 7, pp. 1079–1107.
5.“Hierarchical watermarking for secure image authentication with localization (Jun 2002),” IEEE Trans. Image Process., Vol. 11, No. 6.
6.National Electrical Manufacturers Association (NEMA) (2003), Digital Imaging and Communications in Medicine (DICOM).
7.Ingemar J. Cox, Matt L. Miller and Andrew L. McKellips. “Watermarking as Communications with side information”[A]. Proceedings of the IEEE[C], , 1999, 87(7), pp.1127-1141.
8.HsuChiouting, Wu Jaling. “Multiresolution watermarking for digital images”[J]. IEEE Trans on Circuits and Systems for Video Technology, 1999, 9(4), pp.1097-1101.
9.Marcus J. Nadenau, JulienReichel, , and Murat Kunt. “Wavelet-Based Color Image Compression: Exploiting the Contrast Sensitivity Function”[J]. IEEE transactions on image processing, January 2003, Vol. 12, No. 1.
10.M.D Swanson, M.kobayashi and A.H Tewfik and A.Lu. “Techniques for data hiding”[A]. Proceedings of the IEEE[C], June 1998.