An SVD Based Fragile Watermarking Scheme Tamper Localization and Self Recovery

T.J.Jeyaprabha M.E [1], G.Rajeswari [2]
[1]*Assistant Professor/ Department of ECE, Sri Venkateswara College of Engineering, Tamilnadu 602117*
[2]*PG Student/ Department of ECE, Sri Venkateswara College of Engineering, Tamilnadu 602117*

***Abstract*— This paper proposes an biometric identification system using data hiding and fingerprint recognition.Recently, the medical image has been digitized by the event of computing and digitization of the medical devices. There are needs for database service of the medical image and future storage due to the development of standards, telemedicine, and et al. Furthermore, authentication and copyright protection are required to guard the illegal distortion and reproduction of the medical information data. During this paper, we propose digital watermarking technique for medical image that forestalls illegal forgery which will be caused after transmitting medical image data remotely. A wrong diagnosis could also be occurred if the watermark is embedded into the entire area of image. Therefore, we embed the watermark into some area of medical image, except the choice area that creates a diagnosis so called region of interest (ROI) area in our paper, to extend invisibility. The watermark is that the value of bit-plane in wavelet transform of the ROI for integrity verification. The bit plane image encryption scheme is proposed for encryption of watermark and implements DWT at fourth level for hiding information using DWT on the duvet image and secret image.**

***Index Terms*— Steganography, watermark, dewater mark, Bit Plane, MSB plane, LSB plane.**

INTRODUCTION

The huge fame gained by the World Wide Web over the past decades proves the commercial promise of presenting multimedia assets over the digital networks. As the commercial benefits look to implement digital networks in an attempt to represent digital media to get benefits, they maintain to possess a great interest in guarding the rights of ownership, and digital watermarking has been one of the solutions to this proposition so far. Protection of the copyright has been one of the problematic issues digital images have had, one that has made a lot of problems for the media [1]. In addition, data has the ability to be transferred in many ways like the formats of image, text, audio and video. As the data is being transmitted over a long distance range, illegal users may receive the data or try to manipulate it. Therefore, the authorized users may lose their data and because of this matter the issue of copyright protection has been brought up.

Digital watermark is a type of digital pattern or signal that it injected inside a digital image in an attempt to protect its ownership rights on digital, video, audio and image data. On the other hand, it can be employed to detect the digital documents that have been distributed illegally. In current years, the concept of digital watermarking has gained popularity because of its vast range of usage in the authentication of the contents and protection of the digital multimedia data`s legal ownership.

Digital image watermarking can be classified into two main groups in regard to its domains of embedding that divided into frequency domains and spatial domains. Over the spatial domain, a watermark can be embedded to a host image by modifying the gray levels for some of the pixels of the host image, even though this data can be easily traced via computer analysis. Figure 1 shows various bit-planes of a digital image, where the watermark can be embedded. As it can be understood, when the rate for bit-planes (N) is which is implemented for watermarking rises, the watermarked image gets to be clearer. Therefore when we put 8 bit-planes, (N=8), the watermarked image will be completely perceptible.

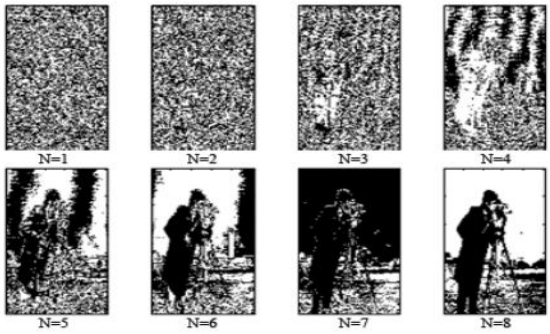

Figure 1. Different 8 bit-planes of a watermarked image

In the second class, that is frequency domain, watermark will be embedded inside transformed images` coefficients. Here we have a number of algorithms at hand like DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform) and DFT (Discrete Fourier Transform). As an example, a DCT has the ability to express a group of cosine capacities that can oscillate at various frequencies that involves a finite sequence of a big number of data points.

Watermarking biometric data is a still a relatively new issue, but it is of growing importance as more robust methods of verification and identification are being used. Biometric provide the necessary unique characteristic but their validity must be ensured. This can be guaranteed to an extent by watermarks. In our Research , Image Watermarking using Least Significant Bit (LSB) algorithm is used. Proposed algorithm performs preprocessing operation on fingerprint & digital signature images. Often by isolating particular bits of pixel value in an image, I have highlight interesting aspects of that image. Higher order bits usually contain most of the significant visual images & lower order bits contain subtle details. This work has been implemented through MATLAB.

LITERATURE REVIEW

A pseudorandom number sequence or chaotic sequence is used for generating a watermark. The digital ownership of a watermark is an issue that has not been addressed in the present methods. In case of piracy of the digital media will be difficult to prove ownership of a digital watermark [1] . The dispute of ownership for digital media will define it is not physically owned. Digital ownership is the solution for the copyright protection for digital media. A watermarking will be present permanently in the original data. Even when the data has a circulation and reproduction [2]. The watermark implanted regions are selected in the high energy regions. It makes the embedded image robust against signal processing attacks. To sustain the processing attacks and to be secure the watermark needs to have the requirements of perceptual transparency and robustness. Perceptual transparency means that the visibility of an image is not changed due to a watermark embedded in the host image [3]. Robustness means the implanted watermark survives even when the image undergoes through signal processing attacks like histogram, filtering etc. Only Authorized persons should be able to detect the watermark image [4]. when two or more images are spliced together to create convincing image forgeries, geometric transformations, such as resizing and rotation, are almost always needed. In recent years, researchers have developed many digital forensic techniques to identify these operations [5].

Previous works in this area focuses on the analysing of images that have undergone single geometric transformations, e.g., resizing or rotation. In several recent works, researchers have addressed yet another practical and realistic situation: successive geometric transformations, e.g., repeated resizing, resizing-rotation [6]. The biometric system can be roughly sketched and consists of a sensor module, a feature extractor module, a matcher, a database, and an application device which is driven by the matcher output. In a feature transformation approach, a function that is dependent on some identification parameters, which can be used as a key an it is applied to the input biometric to generate the protected templates. The employed function can be either invertible, resulting in a salting approach. When a one-way function is applied to the template and it is computationally hard to invert the function even if the transformation parameters are known [7] .

WATERMARKING SCHEME

In proposed system, we applied the modified discrete wavelet transform (DWT), where the watermark was a random bit sequence. The embedding was based on

combining expanded bit multi-scale quantization technique with adjusted watermarked location. The watermark was extended into three bits and insert in the low-frequency sub-bands of the second level DWT decomposition. At the received side, they divided the image into 3×3 size, and then a modified authentication method was achieved, which scans the generated watermark bit matrix. Then, after the watermark extraction, we calculated the PSNR between the original watermark and the extracted one.

Image Preparation

We use some 8-bit grayscale ultrasound images with 640x480 pixels resolution in bitmap format. The sample images are downloaded from www.ultrasound-images.com. First, an image is divided into ROI and RONI. Watermarking for tamper detection and recovery process will be done in ROI. RONI will be used to embed the original LSBs of the image so the watermark can be reversible. We embed all LSBs of the image instead only LSB from ROI. To make it general for all of our sample images, we use static size of ROI and RONI as shown in the figure below.

Fig. 1 Location of ROI and RONI

ROI is defined as a rectangle around the center of the image. The ROI will be divided into blocks of 6x6 pixels. We use smaller 6x6 pixels block size instead of 8x8 pixels to achieve better accuracy of tamper localization an better quality of recovered image [5]. We need to prepare a one to one block mapping sequence AÆBÆCÆDÆ…ÆA for watermark embedding in ROI, where each symbol denotes an individual block. The recovery information of block A will be embedded in block B, recovery information of block B will be embedded in block C, and so on.

$$\vec{B} = [(k \times B) mod N_b] + 1 \qquad (1)$$

where B, , k [1, Nb] , k is a prime number, and Nb is the total number of blocks in the ROI. Each block in the ROI is assigned with an unique integer B {1, 2, 3, ..., Nb }. In this scheme, raster scan (left-right top-bottom) is used to assign number to each block. RONI is later divided into 6x1 pixels blocks. After the original LSBs is compressed using RLE, each resulting RLE package will be embedded in a block in RONI.

Watermark Embedding and Retrieval

Watermark embedding process and extraction process are shown in Fig. 1 and 2 respectively. The proposed method is simple to apply, robust to different attacks and, has good fidelity to HVS. Broadly, in this method, original image and watermark are decomposed in to bit planes. Combinations of significant bit planes are searched to obtain optimal bit plane combination. Finally, using the identified bit planes watermarking is carried out. In this proposed method, let X(m,n) be the grey level image and W(m,n) be the original digital signature. watermark. The grey level image is transformed into the watermarked imageY (m,n) W . The grey scale image X is defined as follows: X ={X(m,n), m∈ 1{ ,.....,M}, n∈ 1{ ,.....,N}} , and M, N are maximum dimensions of an image, where X(m,n)∈ 0{ ,.....,..255} total number of grey levels. Step by step algorithm for proposed method is explained below:

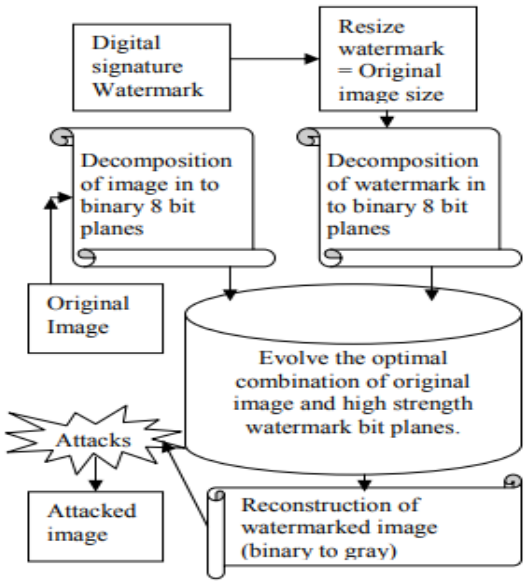

Fig. 1 Watermark embedding process

Step 1: Decompose the grey level image to bit planes: Grey level image is decomposed in to bit plane image. Each pixel in the image is represented by 8-bits. Therefore the image is decomposed into eight 1-bit planes, ranging from 8th bit plane for LSB to 1st bit plane for the MSB. The 8th bit plane contains all the lowest order bits in the pixels comprising the image and 1st bit plane contains all the higher order bits as shown in Fig. 3. Fig. 4a and 4b show grey level original image and digital signature watermark of dimension 256 x 256 respectively. These are decomposed in to bit planes as follows. Decomposition of original image in to 8-bit planes (refer Fig. 2):

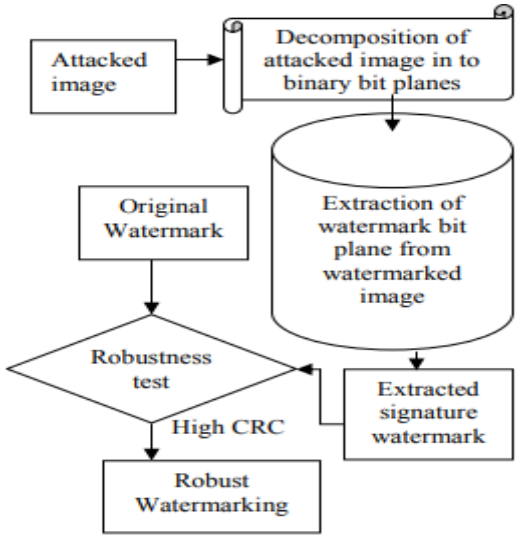

Figure 2 Watermark extraction process

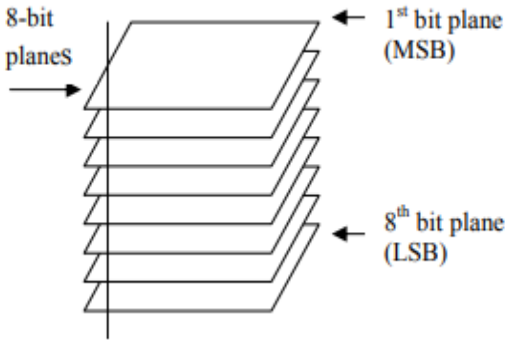

Fig. 3. Bit plane representation of an image

Step 2: Replace the significant bit plane of original image with watermark bit plane: Following set of equations display replacement of 7th bit plane of original image with 1st bit plane of digital signature watermark as an example. The same procedure can be adopted for the remaining bit planes of the image.

$$Y_{b1}(m,n) = X_{b1}(m,n)$$
$$Y_{b2}(m,n) = X_{b2}(m,n)$$
$$\text{-----}$$
$$\text{-----}$$
$$\text{-----}$$
$$Y_{b7}(m,n) = W_{b1}(m,n)$$
$$Y_{b8}(m,n) = X_{b8}(m,n)$$

Resultant watermarked image is as follows:

$$Y_W(m,n) : Y_W(m,n) = Y_{b1}(m,n) + Y_{b2}(m,n) + \ldots\ldots\ldots + Y_{b8}(m,n)$$

This bit plane watermarked image YW (m, n) is recomposed in to grey level image I(m,n).

Step 3: Selection of significant bit planes of original image for watermarking: Fig. 6 shows watermark embedded in all eight bit planes of original image by step 2. This is done so as to decide, by HVS, which bit planes of the image are good for watermarking. The bit plane, which does not degrade the image quality, after embedding watermark, is desirable. Accordingly the LSB (8th bit plane) and the one previous to LSB (7th bit plane) are most suitable as image quality is not degraded after watermark embedding. Therefore these bit planes shall provide good fidelity hence, selected for further analysis.

Step 4: Formulation for watermarked image subjected to attacks: In real life when watermarked image is distributed on the World Wide Web, it is encountered by different attacks. In this step, watermarked image is subjected to ten different types of attacks, leading to attacked image:

$$I_i^*(m,n), i \in \{1,2,\ldots,10 \quad different \quad attacks \quad\}$$

$$I_i^*(m,n) = I_1^*(m,n), I_2^*(m,n), \ldots\ldots\ldots I_i^*(m,n)$$

Step 5: Watermark Retrieval: In this step attacked image (,) * Ii m n is again transformed in to binary image i. e. 8-bit planes as shown below.

$$I_{il}^*(m,n) = I_{ib1}^*(m,n) + I_{ib2}^*(m,n) + \ldots\ldots\ldots\ldots + I_{ib8}^*(m,n)$$

Step 6: Computation of CRC: Correlation coefficient between retrieved watermark and original watermark is estimated using a standard equation (6). The estimated correlation coefficients are denoted asCRCi l,(k) . Where, I indicate different attacks, l is taken as 7th and 8th bit planes of original image as selected in step 3 and k denotes the bit planes of watermark from 1 to 8. The quality of watermarked image is observed by HVS. CRC varies between 0 and 1. CRC is defined as given below:

$$CRC = \frac{\sum_{n=1}^{256}\sum_{m=1}^{256} W(m,n)\times W^{*}(m,n)}{\sqrt{\sum_{n=1}^{256}\sum_{m=1}^{256} W(m,n)\ \sum_{n=1}^{256}\sum_{m=1}^{256} W^{*}(m,n)}}$$

$$if\ CRC_i(l,k) = \begin{cases} 0, & less\ robust\ watermarking \\ 1, & highly\ robust\ watermarking \end{cases}$$

Step 7: Estimation of peak signal to noise ratio (PSNR): PSNR is calculated by using following equation. Capacity of the original image to carry the watermark is computed by measuring PSNR, which is defined as follows:

$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE} (db)$$

Mean square error is defined as:

$$MSE = \frac{1}{(m\times n)} \sum_{n=1}^{256}\sum_{m=1}^{256} (W(m,n) - W^{*}(m,n))^2$$

Where W(m,n) is the original watermark, * W m n is the extracted watermark after attack.

Step 8: Weighted correlation coefficient computation: Weighted correlation coefficient is defined as follows:

$$Wt.\ CRC\ (l,k) = \sum_{i=1}^{10} CRC\ _i(l,k)\times a_i$$

Where, ai are the different weightings of attacks such that total 1 ai =a1 +a2 +———+a10 = , and i is the number of attacks. The identified attacks are assigned weightings based on damage caused, frequency, intensity and criticality or any other such criterion by the user. Based on these weightings, considering all the ten attacks, weighted correlation coefficient are estimated, for each bit plane combination of image and watermark under consideration. The step is repeated for combinations of selected bit planes of image and the entire bit planes of watermark respectively.

Step 9: Optimization: The above step 8 is repeated by varying the weightings of attacks. The bit plane combination of original image and watermark for which, the weighted correlation coefficient is maximum, is selected as the optimized one for the given user requirements. This combination is used for optimized watermarking in terms of robustness and fidelity.

EXPERIMENTAL RESULTS

We have implemented our method on still grey scale image (dimension 256 ×256). In the subsections to follow extensive analysis is carried out to evolve the optimal combination of bit planes (image and watermark) to achieve desirable properties after watermarking.

Fig 4. Biometric Key

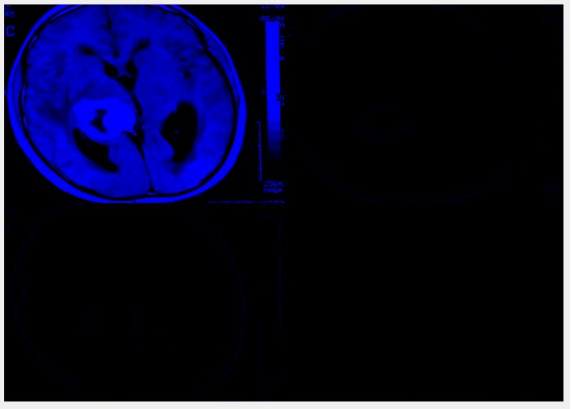

Fig 5. Bitplane Slicing

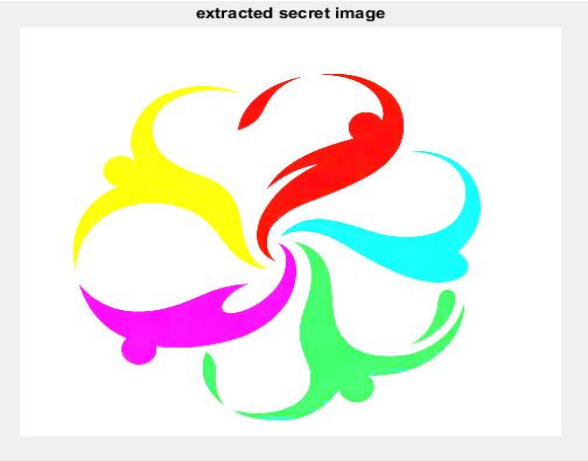

Fig 6. Water Mark Extraction

Table 1: Quality Measurements

sr no.	Image name	PSNR	MSE
1	D_1.jpg	18.8359	850.1401
2	D_2.jpg	18.1576	993.8458
3	D_3.jpg	17.1881	1.24E+00
4	D_4.jpg	17.747	1.09E+03
5	D_5.jpg	19.0108	816.5761
6	D_6.jpg	18.6838	880.4443
7	D_7.jpg	19.0876	802.2744
8	D_8.jpg	19.0876	802.2744
9	D_9.jpg	18.93273301	8.31E+02
10	D_10.jpg	18.99452271	8.20E+02

CONCLUSION

Reversible image watermarking using bit plane coding is done and is completely reversible. Arithmetic coding used for compression guarantees complete reversibility. Lower bit planes have lower embedding capacity but since they are less significant for visual perception image quality is better than in higher bit planes. Performances of various wavelet families are studied. Bior 3.3 and cdf 9/7 perform better than other wavelets for this algorithm. Hash of the images were embedded and tested for authentication and security. The first bit-plane is the least significant one (LSB) and most of the time is hardly related to the main shapes of the picture. On the other hand, the last bit-plane is the most significant one (MSB) and contains the main lines and edges of the picture. The resulting watermarked image has a good quality and the watermark is imperceptible. Referring to results shown in Table 1, it can be concluded that proposed method leads to robust watermarking against geometric attacks and also yields highest correlation coefficient as compared to the previous bit plane method and other combination of bit planes. Also, it can be noted that PSNR value for proposed method is higher i. e. above 87 db.

REFERENCES

[1] A. K. Pal and T. Pramanik, "Design of an Edge Detection Based Image Steganography with High Embedding Capacity," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Quality, Reliability, Security and Robustness in Heterogeneous Networks, pp. 794800, 2013.

[2] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," Information Sciences, vol. 279, pp. 251272, 2014.

[3] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9- 10, pp. 16131626, 2003.

[4] R. Chowdhury, D. Bhattacharyya, S. K. Bandyopadhyay, and T.-H. Kim, "A View on LSB Based Audio Steganography," International Journal of Security and Its Applications, vol. 10, no. 2, pp. 5162, 2016.

[5] M. Averkiou, "Digital Watermarking," Cambridge: University of Cam-bridge, 2009.

[6] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia dataembedding and watermarking technologies," Proceedings of the IEEE, vol. 86, no. 6, pp. 10641087, 1998.

[7] M.Q. Chen, X.X. Niu, Y.X. Yang, "The research developments and applications of digital watermarking," J. China Inst. Commun. 22 (5): 71-79, 2001.

[8] Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and S. Naha-vandi, "PatchworkBased Audio Watermarking Method Robust to De-synchronization Attacks," IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 22, no. 9, pp. 14131423, 2014.

[9] C. Rey and J.-L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication," EURASIP Journal on Advances in Signal Processing, vol. 2002, no. 6, pp. 613621, 2002.

[10] V. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," INDIN '05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.

[11] S. Liping, Q. Zheng, L. Bo, Q. Jun, and L. Huan, "Image scram-bling algorithm based on random shuffling strategy," 2008 3rd IEEE Conference on Industrial Electronics and Applications, 2008.

[12] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing, vol. 66, no. 3, pp. 385403, 1998.

[13] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible Image Watermarking Using Interpolation Technique," IEEE Transactions on

Information Forensics and Security, vol. 5, no. 1, pp. 187193, 2010.

[14] X.-T. Wang, C.-C. Chang, T.-S. Nguyen, and M.-C. Li, "Reversible data hiding for high quality images exploiting interpolation and direction order mechanism," Digital Signal Processing, vol. 23, no. 2, pp. 569577, 2013.

[15] X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," Signal Processing, vol. 93, no. 1, pp. 198205, 2013.

[16] N. S. T. Sai and R. C. Patil, "Image Retrieval using Bit-plane Pixel Distribution," International Journal of Computer Science and Information Technology, vol. 3, no. 3, pp. 159174, 2011.