Robust and indiscernible multimedia watermarking using light weight mutational methodology

Rayi Sailaja[1,*], Ch Rupa[2], A.S.N Chakravarthy[3]

1. Dept. of CSE, Aditya College of Engineering and Technology, Surampalem, India

2. Dept of CSE, VR Siddhartha Engineering College, Vijayawada, India

3. Dept of CSE, JNTUK-UCEV, Vizianagaram, India

sailajarai@gmail.com

ABSTRACT. *In recent years, with the growing use of the internet and wireless networks, the exchange and access to multimedia data through the insecure web is also growing as a part of telemedicine. Using the concept of multimedia watermarking, the proposed system aims at providing authentication, confidentiality, and integrity to the patient medical record. A new robust and imperceptible watermarking approach is proposed which is based on a mutational encryption, lifting wavelet transform and singular value decomposition for authenticating medical images. To provide authentication and confidentiality, patient data is encrypted with mutation algorithm and embedded in a patient fingerprint image using Penultimate Least Significant Bit (PLSB), Then the fingerprint image is watermarked into a medical image using an LL band of the cover image and the HH band of watermark image obtained by second level LWT and SVD. The proposed approach performance is assessed by different image quality metrics. The watermarked image quality and extracted watermark image quality are analyzed at different scaling factors with the help of Normalized correlation and Peak signal to noise ratio. Investigation results exhibit that the proposed approach can withstand different image processing attacks like a Median filter, JPEG compression, Gaussian, Salt, and pepper Noise. So the proposed work can be used to transmit a patient's multimedia medical data by providing high security and privacy.*

RÉSUMÉ. *Ces dernières années, avec l'utilisation croissante d'Internet et des réseaux sans fil, l'échange et l'accès aux données multimédia via le Web non sécurisé se développent également dans le cadre de la télémédecine.En utilisant le concept de filigrane multimédia, le système proposé vise à fournir une authentification, une confidentialité et une intégrité au dossier médical du patient.Une nouvelle approche de filigrane robuste et imperceptible est proposée, basée sur un cryptage mutationnel, une transformation en ondelettesde levage et une décomposition en valeurs singulières pour l'authentification des images médicales.Pour assurer l'authentification et la confidentialité, les données du patient sont cryptées avec l'algorithme de mutation et incorporées dans une image d'empreinte digitale du patient à l'aide du Penultimate Least Significant Bit (PLSB). L'image de l'empreinte digitale est ensuite filigranée dans une image médicale en utilisant une bande LL de l'image de couverture et le*

HH bande de l'image en filigrane obtenue par LWT et SVD de deuxième niveau.La performance de l'approche proposée est évaluée par différentes métriques de qualité d'image.La qualité d'image en filigrane et la qualité d'image extraite en filigrane sont analysées à différents facteurs de mise à l'échelle à l'aide de la corrélation normalisée et du rapport signal / bruit de pointe.Les résultats de l'enquête montrent que l'approche proposée peut résister à différentes attaques de traitement d'image telles qu'un filtre médian, une compression JPEG, un bruit gaussien, sel et poivre. Ainsi, le travail proposé peut être utilisé pour transmettre les données médicales multimédia d'un patient en offrant une sécurité et une confidentialité élevées.

KEYWORDS: *three lines maximum, lifting wavelet transform, singular value decomposition, peak signal to noise ratio, normalized correlation.*

MOTS-CLÉS: *trois lignes maximum, Transformation en ondelettes de levage, décomposition en valeurs singulières, rapport signal / bruit de pointe, corrélation normalisée*.

DOI:10.3166/TS.34.45-55 © 2017 Lavoisier

1. Introduction

There is a tremendous increase in distributing digital medical images through the internet for accurate diagnosis by different specialists. Treatment can be obtained for serious health issues without roaming around the world with the help of Telemedicine. With the aid of Telemedicine patient, medical history and reports can be sent over the internet so that doctors around the world can perform diagnosis using those reports. However, unsecured transmission, storage, and electronic patient data over the internet is the most vital issue in this field. Medical images contain very sensitive health data, So it became necessary to secure medical images from unauthorized access and tampering. Medical identity theft is also budding these days as reported in the various surveys (Bowman, 2012; Ollove, 2014).

Medical Image watermarking can be used to serve the purpose of transferring the medical history of a patient through the web. Patient details can be embedded in the medical images in encrypted form. At the receiving end, it can be extracted and decrypted to verify the patient details. Through medical image watermarking patient information is maintained confidentially. The proposed approach provides authenticity and integrity for the content of the medical image.

Digital watermarking is the practice of inserting watermark signal information into the host image, this watermark signal can be extracted at the receiver for different purposes like authentication, copyright protection, Content identification, integrity, etc.

Medical image watermarking needs extreme care, such that it does not impact the image quality when patient information is inserted into the medical images. The major security concern when the patient data is exchanged through the web is authentication, confidentiality, availability, and integrity (Kumar *et al*., 2012; Mohanty, 1999). Singh *et al*., (2015) proposed an algorithm which embeds patient information into chosen sub-band of Discrete wavelet transform coefficients of the reference medical image using a spread spectrum technique. It is observed that the watermark is extracted with high robustness and shown better results against different attacks.

Nayak *et al.,* (2004) proposed a technique in which patient data is encrypted and manipulated with error control codes. These coded data bits were exchanged with the LSB of the gray image pixel value. Bit error rate (BER), the percentage of distortion and the number of characters modified are evaluated for different signal to noise ratio. In this work, authors have applied only salt and pepper noise attack to check the robustness of the interleaved image.

Anand and Natarajan (1998) proposed an algorithm which encrypted patient data and watermarked into medical images by exchanging the least significant bits of the gray values of selected pixels of the original reference image with a watermark image. But the author does not analyze the efficiency of the proposed work with image processing attacks.

Nambakhsh *et al.,* (2006) presented a watermarking approach in which the zero-tree wavelet algorithm is used. The proposed approach performance is evaluated on various CT and MRI images and also claimed that it uses only 15% of the host image to insert watermark signal.

Lavanya and Natarajan (2012) proposed a technique in which patient data is embedded into the encrypted image. It is shown that the medical image is encrypted and regions of noninterest are selected and patient data is embedded into it. The embedded data is recovered successfully and its embedding capacity is more. But its robustness is not analyzed against different processing attacks.

Mohammad and Elyadem (2014) proposed a method in which image is divided into groups and their R-S vectors are compressed and also SHA 256 algorithm is applied and its hash value is generated which is encrypted along with compressed R-S vector and patient ID using RSA. The encrypted code is watermarked into the original image. Its experimental results show that its embedding capacity is 0.525bpp.

Zang and Huang (2013) presented a medical image authentication which uses chaos. It is shown that it has a highly stable signal to noise ratio. Mohammed Ibrahim (Khan *et al.,* 2013; Lai and Tsai, 2010; Umamaheswari and Thanushodi, 2012) propped different wavelet related watermarking approaches for medical images.

This paper presents a robust watermarking approach which provides both authentication and confidentiality to the patient medical data by encryption. Here we have used a lightweight mutational encryption which converts plaintext into a form which is easily storable in a watermark image by penultimate and least significant bit method. This watermark image is embedded into the original image using LWT-SVD based watermarking algorithm. When compared to other approaches the proposed approach provides robustness against different image processing attacks like jpeg compression attacks, median filter attack, Gaussian noise attacks, salt, and pepper noise attacks and also meets the security requirements like authentication, confidentiality. The present approach successfully extracts the watermark image and encrypted data. This approach is very much useful for medical practitioners who want to study the patient's health condition from a distance.

The proposed approach is organized as follows; Performance measures are discussed in Section 2. Section 3 describes the proposed work in detail. Experimental results were shown in section 4.

2. Performance measures

Different image quality metrics are available which compare the original image and the distorted image. The most extensively used and simple image quality metric is the mean square error (MSE) which is evaluated by averaging the squared differences of distorted and reference image pixels. MSE value is used to evaluate peak to signal noise ratio (PSNR). A larger PSNR indicates more imperceptibility and is defined as

$$\mathrm{PSNR} = 10\log\frac{(\mathrm{Bmax})^2}{\mathrm{MSE}} \tag{1}$$

MSE can be computed as

$$\mathrm{MSE} = \frac{1}{\mathrm{P}\times\mathrm{Q}}\sum_{\mathrm{i}=1}^{\mathrm{P}}\sum_{\mathrm{j}=1}^{\mathrm{Q}}\big(\mathrm{O}(\mathrm{i},\mathrm{j}) - \mathrm{W}(\mathrm{i},\mathrm{j})\big)^2 \tag{2}$$

where, O(i,j) is the original reference image pixel of size P*Q and W(i,j) is the distorted image pixel. Bmax is the maximum pixel value of the image. As per (Singh, 2014) the PSNR value of higher than 27 DB is acceptable for the watermarked image. The resemblance of the extracted watermark with original watermark can be evaluated using Normalized correlation factor and is computed as

Table 1. Other image quality metrics

S.No	Metric	Description
1	Average Difference	$\mathrm{MD} = \frac{1}{\mathrm{P}\times\mathrm{Q}}\sum_{\mathrm{i}=1}^{\mathrm{p}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\mathrm{O}(\mathrm{i},\mathrm{j}) - \mathrm{W}(\mathrm{i},\mathrm{j})$
2	Structure Content	$\mathrm{SC} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{p}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\mathrm{W}(\mathrm{i},\mathrm{j})^2}{\sum_{\mathrm{i}=1}^{\mathrm{p}}\sum_{\mathrm{j}=}^{\mathrm{q}}\mathrm{O}(\mathrm{i},\mathrm{j})^2}$
3	Normalized Absolute Error	$\mathrm{NAE} = \frac{1}{\mathrm{PQ}}\sum_{1=1}^{\mathrm{p}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\lvert\mathrm{O}(\mathrm{i},\mathrm{j}) - \mathrm{W}(\mathrm{i},\mathrm{j})\rvert$
4	Maximum Difference	$\mathrm{MD} = \mathrm{MAX}\lvert\mathrm{O}(\mathrm{i},\mathrm{j}) - \mathrm{W}(\mathrm{i},\mathrm{j})\rvert$
5	Image Fidelity	$\mathrm{IF} = 1 - \frac{\sum_{\mathrm{i}=1}^{\mathrm{p}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\mathrm{O}(\mathrm{i},\mathrm{j})\times\mathrm{W}(\mathrm{i},\mathrm{j})}{\sum_{\mathrm{i}=1}^{\mathrm{p}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\mathrm{O}(\mathrm{i},\mathrm{j})}$

$$\mathrm{NC} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{p}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\mathrm{O}(\mathrm{i},\mathrm{j})\times\mathrm{W}(\mathrm{i},\mathrm{j})}{\sum_{\mathrm{i}=1}^{\mathrm{P}}\sum_{\mathrm{j}=1}^{\mathrm{q}}\mathrm{O}(\mathrm{i},\mathrm{j})^2} \tag{3}$$

There are other image metrics using which we can analyze the image quality. They are listed in Table 1. Where, O(i,j) refers to the reference image and W(i,j) refers to the distorted image.

3. Proposed approach

In this approach, MRI image is considered as reference host image and the patient fingerprint image is considered as a watermark image. Patient information like name, age, problem, etc is encrypted by Light Weight Encryption and embedded into the fingerprint watermark image using Penultimate Least Significant Bit. The watermark image is watermarked into the original MRI image using LWT-SVD based watermarking algorithm. The proposed approach has been compared with the approach discussed (Singh *et al.,* 2016) and shown better results. Light Weight Encryption.

3.1. Light weight mutation encryption (lwe) algorithm –

1: Read the plaintext 'P' i.e P = p1, p2 ,…, p_m.
Where 'm' = length (P).
2: $X_a = P_{ik}$; where $1 < k \leq 8$ and $1 < i \leq m$ and $a = k * m$
i.e $X_1 = P_{11}$
$X_2 = P_{12}$
…….
….
$X_a = P_{m8}$
3: Loop begin
if (X_a ! = '\') then
Y_b = if (X_a == 0) ? Y_b = '|' : Y_b = '-' ;
where $1 < b \leq a$
end if
4: C_i = if (Y_a == '|') ? ROTL (Y_b ,1) : ROTR(Y_b,1)
where $1 < i \leq a$
5: End loop

3.2. Multimedia embedding method –

In order to provide security for the multimedia data such as text, images, audio, and video, here used indiscernible watermarking embedding method using Penultimate Least Significant bit (PLSB) [16] which has proposed in our earlier work and Light Weight Mutational Encryption (LWE). The proposed embedding and extraction methodology are shown in the Figure 1. As a part of this process, consider the following modules to get the watermarked data.

Module 1: LWE based cipher text embeds into the watermark data by PLSB method (Sailaja et al., 2014) which generates stego multimedia data.

Module 2: Stego multimedia data embeds into the cover data using LWT –SVD (Radhika et al., 2016) that can generate watermarked data.

3.2.1. Application for multimedia embedding algorithm

1: Apply the second level LWT on Cover Image and Watermark Image
[cAc, cHc, cDc, cVc]=lwt2(Cover Image)
[cAw, cHw, cDw, cVw]=lwt2(Watermark Image)
2: Select the subband cAc and cDw and apply SVD.
3: Select the matrices Sc and Sw obtained from above step and mutate using scaling factor α to get Scw
4: Perform Inverse SVD to get cAwk
5: Perform second level ILWT using cAwk, cHc, cDc, cVc to obtain the watermarked image.

3.3. Multimedia extraction approach

Module 1: Apply inverse procedure of LWT – SVD (Radhika et al., 2016) to extract stego multimedia data from the covered data.

Module 2: Extract the ciphertext from the stego multimedia data through PLSB.

3.3.1 Application for multimedia extraction algorithm

1: Apply the second level LWT on Cover Image and Watermarked Image
[cAc, cHc, cDc, cVc]=lwt2(Cover Image)
[cAwk, cHw, cDw, cVw]=lwt2(Watermarked Image)
2: Select the subband cAc and cAwk and apply SVD.
3: Select the matrices Sc and Swk obtained from above step and mutate using scaling factor α to get Scw

$$Scw = (Swk - Sc) / \alpha \quad (4)$$

4: Perform Inverse SVD to get cAw

$$cDw = Uw, *Scw* Vw \quad (5)$$

5: Construct extracted watermark image by performing second level ILWT using cAwk, cHc, cDc, cVc to obtain the watermarked image.

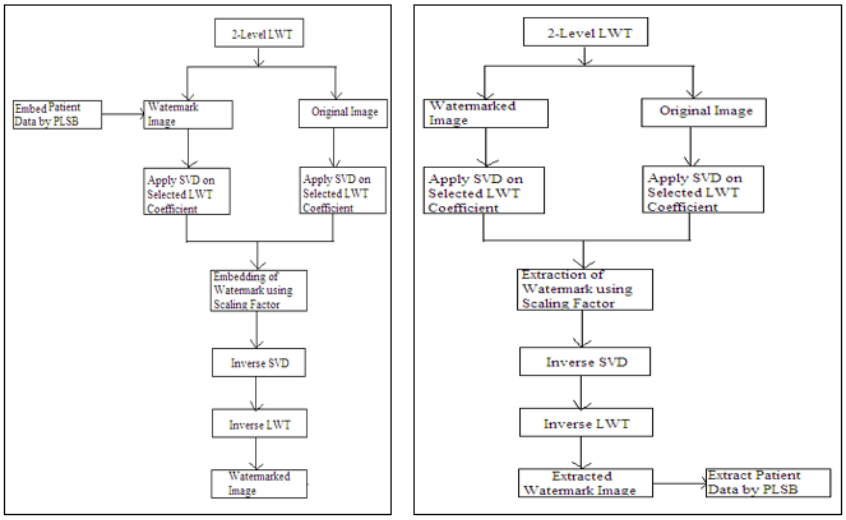


Figure 1. Patient data application for watermarking

4. Experimental results

The major challenges of multimedia content authentication using watermarking are to achieve the parameters like robustness against different image incidental distortions, maintaining the good perceptual quality of the original image and extracted watermark image.

The proposed approach has been tested on text and medical image data using MATLAB R2014a. We tested on MRI brain images around 50 to test the performance of the proposed method. Here we considered that both original and watermark images are 8-bit grayscale images. Their size is considered as 256×256. It is observed that the perceptual quality of the watermarked image is maintained. The watermarked image resembles the original image so the anonymity of the existence of the watermark is maintained successfully.

The perceptual quality of the extracted watermark image and the watermark image is analyzed with image metrics like Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC), Mean Square Difference (MSE), Average Difference (AD), Maximum Difference (MD), Structure Content (SC), and Normalized Absolute Error (NAE) and shown in Table 2.

Ideally, NC value should be 1 but value up to 0.7 is acceptable according to [1] This approach provides NC of 0.999. The acceptable value of PSNR due to wireless transmission quality loss is between 20dB and 25dB, but higher is better. This approach exhibits PSNR above 50dB which indicates that image reconstruction is of high quality. It's Mean Square Error and Average Difference is also small.

Table 2. Proposed approach performance at scaling factor 0.01

Image Quality Metric	Value
Mean Square Error	0.26
Peak Signal to Noise Ratio	54.072
Normalized Correlation	0.999
Maximum Difference	18.000
Structure Content	0.999
Normalized Absolute Error	0.004
Average Difference	0.797

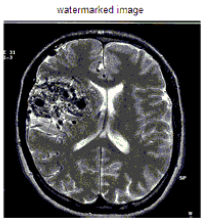
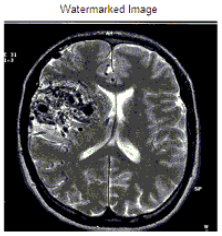
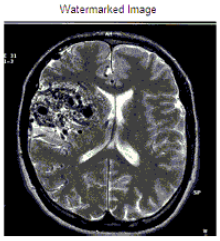
Watermarked image robustness is evaluated by adding intentionally some noise to the watermarked image, whether it is able to resistant to different image attacks like Gaussian noise, median filtering, salt & pepper, JPEG Compression. The approach's performance is evaluated with respect to NC at scaling factor 0.1, also proposed approach is compared with the existing approach (Singh *et al.,* 2016) and shown better results as shown in Table 3.

Table 3. Comparison of NC values of existing and proposed approach

Attacks	Existing Approach	Proposed Approach
Gaussian Noise	0.975	0.999
Median filtering (Mohammad and Elyadem, 2014)	0.998	0.999
JPEG 10	0.990	0.918
JPEG 50	0.978	0.985
JPEG 90	0.998	0.995
Salt and Pepper 0.001	0.963	0.976
Salt and Pepper 0.01	0.755	0.845
Salt and Pepper 0.05	0.606	0.714

The Performance of the proposed approach is also analyzed at different scaling factors and their PSNR, NC, watermarked image and extracted watermark image are shown below in Table 4. We can observe that NC value decreases and PSNR value increases with increase in scaling factor.

Table 4. Performance of the proposed approach at different Scaling factor

Scaling Factor	PSNR	NC	Watermarked Image	Extracted Watermark
0.001	54.758	0.985		
0.01	54.274	0.999		
0.02	52.482	0.999		
0.025	51.593	0.999		

In future, we would like to apply our approach on other types of medical images like CT scan images, X-ray images, etc and compare and analyze their behavior to provide high trust to the patient's ownership.

5. Conclusion

A new robust and secure mutation based medical image authentication approach has been proposed in which patient information is used as the authentication data, is encrypted and embedded into the patient fingerprint image using Penultimate LSB which is considered as a watermark image. Nobody can reproduce the patient's fingerprint image so it authenticates the patient when patient information is successfully decrypted. The watermark image is embedded into an MRI image of the patient using a hybrid approach of LWT and SVD. The proposed method performance is analyzed and verified with respect to different image quality metrics and scaling factors. The proposed approach has shown better results when compared with existing DWT-SVD based approach. So the proposed approach can be used to securely transfer the patient medical history and reports over the web successfully.

Reference

Anand D., Natarajan U. C. (1998). Watermarking medical images with patient information. *Proceeding of IEEE/EMBS Conference*, Hong Kong, China, pp. 703-706. https://doi.org/10.1109/IEMBS.1998.745518

Bowman D. (2012). HTTP:// www.fiercehealthit.com/story/researchers-use-digital-watermarks-protect-medicalimages.

Kabra R. G., Agrawal S. S. (2016). Robust embedding of image watermark using LWT and SVD. *Proceedings of International Conference on Communication and Signal Processing*, No. 6-8, pp. 1968–1972. https://doi.org/10.1109/ICCSP.2016.7754516

Khan M. I., Rahman M. M., Sarer M. I. H. (2013). Digital watermarking for image authentication based on combined DCT, DWT, and SVD transformation. *International Journal of Computer Science Issues*, Vol. 10, No. 5, pp. 223-230. http://www.oalib.com/paper/4039808#.W_9R1fknYcM

Kumar B., Singh H. V., Singh S. P., Mohan A. (2011). High capacity secure spread spectrum watermarking for telemedicine applications. *World Academy of Science Engineering Technology*, Vol. 5, No. 7, pp. 62-66. https://doi.org/10.4236/jis.2011.22009

Lai C. C., Tsai C. C. (2010). digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transaction, Instrum. Meas.*, Vol. 59, No. 11, pp. 3060-3063. https://doi.org/10.1109/tim.2010.2066770

Lavanya A., Natarajan V. (2012). Watermarking patient data in encrypted images. *India Academy of Sciences*, Vol. 37, No. 6, pp. 723-729. https://doi.org/10.1007/s12046-012-0107-z

Mohammad M., Elyadem A. (2014). medical image authentication based on reversible watermarking. *Proceedings of the International Conference on Informatics and Systems*, pp. 15-24.

Mohanty S. P. (1999). Watermarking of digital image. M.S. Thesis, *Indian Institute of Sciences*.

Nambakhsh M. S., Ahmadian A., Ghavami M., Dilmaghani R. S., Karimi-Fard S. (2006). A novel blind watermarking of ECG signal on medical images using EZW algorithm. *28th*

Annual International Conference of the IEEE Engineering in Medicine and Biology Society, No. 1, pp. 3274-3277. https://doi.org/10.1109/IEMBS.2006.259603

Nayak J., Bhat P. S., Kumar M. S., Acharya R. (2004). Reliable transmission and storage of medical images with patient information using error control codes. *Proceeding of IEEE INDICON*, pp. 147-150. https://doi.org/10.1109/INDICO.2004.1497726

Ollove M. (2014). www.usatoday.com/story/.../tateline-identity-thefts-medical.../5279351.

Sailaja R., Rupa C. H., Chakravarthy A. S. N. (2014). A fusion of PLSB and SVD based image watermarking approach. *Proceeding of National Conference on Emerging Research Trends in Computer Science, Also Published in International Journal of Advanced Computer Communications and Control*, Vol. 02, No. 2, pp. 89-91.

Singh A. K., Dave M., Mohan A. (2014). Hybrid technique for robust and imperceptible image watermarking in DWT-DCT-SVD domain. *National Academy of Sciences*, Vol. 37, No. 4, pp. 351-358. https://doi.org/ 10.1007/s40009-014-0241-8

Singh A. K., Dave M., Mohan A. (2016). Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Springer Science Business Media, Newyork, Multimedia Tool and Applications*, Vol. 75, No. 14, pp. 8381–8401. https://doi.org/10.1007/s11042-015-2754-7

Singh A. K., Kumar B., Dave M., Mohan A. (2015). Robust and imperceptible spread spectrum watermarking for telemedicine applications. *Proceeding of National Academy of Sciences, India Section A: Physical Sciences*, Vol. 85, No. 2, pp. 295-301. https://doi.org/10.1007/s40010-014-0197-6

Umamaheswari A., Thanushodi K. (2012). High performance and effective watermarking scheme for telemedicine applications. *Eur Jci Res*, Vol. 67, No. 2, pp. 283-293.

Zang L. H., Huang L. Y. (2013). A research on the medical images authentication watermark method based on chaos. *Proceedings of International Conference on Mechatronic Science Electrical Engineering and Computers*, pp. 1679-1683. https://doi.org/10.1109/MEC.2013.6885328