ISBN 978-93-84468-20-0
Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015)
Singapore, March 29-30, 2015, pp. 82-88

Encryption Based Medical Image Watermarking against Signal Processing Attacks

Abhilasha Sharma[1], Mayank Dave[2], Amit Kumar Singh[1], and S P Ghrera[1]

[1]Department of Computer Science & Engineering, Jaypee University of Information Technology, Waknaghat, Solan Himachal Pradesh India

[2]Department of Computer Engineering, NIT Kurukshetra, Haryana India

Abstract: *The protection of data is of at most importance in the medical field to boost the telemedicine applications. There is a need of robust and secure mechanism to transfer the medical images over the Internet. The algorithm proposed in this study is the watermarking technique in the transform domain to ensure secure transfer of medical data. Using DWT transformation and substitution method, we embed the watermark into the cover image and the watermarked image is then encrypted by using the symmetric stream cipher techniques. Performace of the proposed algorithm is analyzed against various signal processing attacks like compression, filtering, noise and histogram equalization and desired outcome is obtained without much degradation in extracted watermark and watermarked image quality.*

Keywords: *Watermarking, DWT, Robustness, Medical images, Imperceptibility*

1. Introduction

The growing technology nowadays offers substantial new opportunities for sharing and transmission of the valuable digital data such as images, audio and video [1].The Internet and electronic media has improved medical facilities in the form of tele-medicine, tele-diagnosis, tele-consultancy etc. [2]. The digital revolution has boosted the sharing of medical images and confidential medical data among the health care professionals and healthcare institutions, which has led to the requirement of the safety issues concerned with the legal and ethical aspects specific to the medical domain. The ease by which digital data can be duplicated and distributed has raised the need of the effective content and copyright protection mechanisms [3].

With these evolutionary technologies, the security of the medical images and medical records has attracted great attention. The digital handling of such information requires a systematic content validation, copyright management and content protection. The ease of transmitting and sharing the medical data increases the security issues in terms of confidentiality, availability and reliability [4]. The traditional cryptographic techniques provide medical data protection and authentication. Some techniques also provide the confidentiality, integrity and non-repudiation [5-9]. However, only the cryptographic solutions are not sufficient to handle all facets of security in the medical domain [10].

The digital imaging and communication in medicine (DICOM) standards make exchange of medical images more convenient, quicker and dependable. The DICOM files are switched between the entities in a fixed way. Nevertheless, if the cryptanalyst is able to obtain the information regarding key and forms in the encrypted data, the data is no longer protected [11-14]. A method to enhance the security of the medical images is the digital image watermarking [15]. These methods provide the complementary security for the medical images to share them over the open network channels [16, 17]. It is the process of embedding data, called a watermark, to the

multimedia objects such as image, audio, video, etc. Such embedded watermarking can be detected later to make assertions about the objects [18-21].

The main objectives considered in medical applications for the protecting the data are data hiding, integrity control and authenticity [22]. Watermarking provides a novel approach to achieve these characteristics during transfer of data from one host to another. The watermarking can be performed in both spatial and transform domains. In transform domain, the watermark is embedded in the image by modifying the transformation coefficients.

2. Terminology

The proposed work based on Discrete Wavelet Transform (DWT) and stream cipher requires certain theoretical considerations related to and their application in image processing. Hence, a brief description of these concepts is included in the given below sections.

2.1. DWT

DWT provides the multi-resolution analysis having time-frequency location properties, which decomposed the image into a set of four non-overlapping sub-bands. We are using use the Haar wavelets, which are a series of averaging and differencing operations on discrete time signal. An image is transformed into four sub-bands named as LL, LH, HL, and HH. The HH sub-band represents the finest scale coefficients and the LL sub-band represents the coarse level coefficients.

2.2. Stream Cipher

Stream cipher encrypts bits individually, achieved by adding a bit of a key stream of plain text to ensure the privacy on a communication network. These are synchronous cipher techniques, uses the pseudo-random function as key generator. The generated key is used as the one time pad (OTP) and used for encryption masking with the plain text using bitwise XOR operation. The decryption process is done in the same manner, by using the bitwise XOR operation on the cipher text and the pseudo random key.

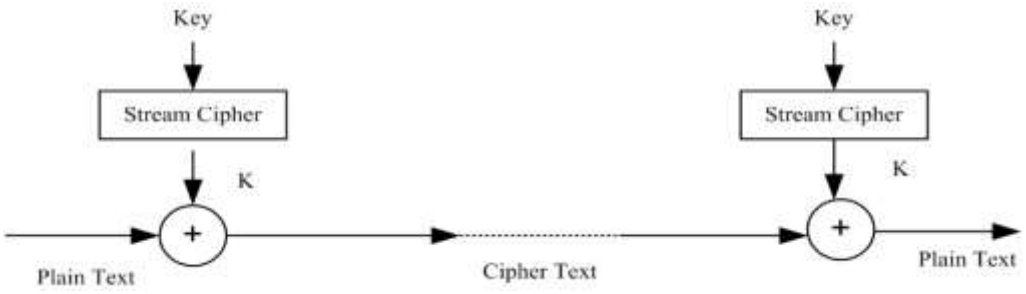

Fig. 1: Stream Cipher

3. Proposed Algorithm

In our proposed method, the watermark and cover images are transformed using Haar wavelets. The watermark image to be embedded is formatted to form the watermark key using modulus functions. To embed the watermark, a bit-plane is selected in the cover image and embedding is done on the selected bit-plane. To enhance the protection of the watermarked image, it is enciphered utilizing the stream cipher symmetric key techniques.

3.1. Embedding Watermark

The first step is to convert the watermark and cover image to grayscale images. Next, we apply 1-level DWT to watermark image ‘W’ to obtain the sub-bands LL, LH, HL and HH. We then apply 1-level DWT to the cover image ‘C’ to obtain the sub-bands LL, LH, HL and HH. Select the LL sub-band of the watermark image and

format using the modulus function to obtain the watermark key. Select the bit-plane to hide the image. Using the selected bit-plane, embed the watermark to the 'LL' sub-band on the cover image 'C'. The watermarked image is encrypted using the stream cipher (RC4) in the transform domain. The watermark embedding process is described in the algorithm given below:

Embedding algorithm for watermark image

Input: The cover image 'C' of size N×N.
The watermark image 'W' of size M×M.

Output: The watermarked image 'Wd' of size N×N

Step1: Perform DWT on Cover and Watermark image
Apply DWT to cover image 'C'
$LL_c \leftarrow$LL band of C
Apply DWT to watermark image 'W'
$LL_w \leftarrow$LL band of W

Step 2: Select the size of the LL sub-band
$C_n, C_m \leftarrow$Size of LL_c
$W_n, W_m \leftarrow$Size of LL_w

Step 3: Format the watermark
Repeat for each value (i,j) of LLw
do
$K(i,j)=LL_w((i \bmod W_n)+1, (j \bmod W_m)+1)$
end
until $i, j \leq C_n$

Step 4: Select the bitplane
Repeat for each value (i,j) of LL_c
do
B= get bit of (i,j)
end
until $i, j \leq C_n$

Step 5: Embedd the watermark to selected bitplane
Repeat for each value (i,j)
do
$W_d(i,j)=setbitto(LL_c(i,j), B, LL_w(i,j))$
end
until $i, j \leq C_n$

Step 6: Encrypt the watermark
Repeat for each value (i, j)
do
E(i,j)= Encrypt(W(i,j))
end
until $i, j \leq C_n$

3.2. Watermark Extraction

Select the encrypted watermarked image. Decrypt the image using the stream cipher, opposite to encryption. Obtain the embedded watermark by extracting using the selected bit plane. The watermark extraction process illustrated in the algorithm given below:

Extraction Algorithm for Image Watermark:

Input: Encrypted watermarked image of size C_n

Output: Watermarked image of size M×M

Step 1: Decrypt the watermark

Repeat for each value (i,j)

do

D(i,j)= Decrypt(E(i ,j))

end

until i,j ≤ C_n

Step 2: Extract the watermark from the selected bit plane

Repeat for each value(i,j)

do

W(i,j)=getbit(D(i,j), B)

end

until i, j ≤ C_n

Step 3: obtain the original image

Rescale W(i,j) to M×M

4. Experimental Results and Discussion

The watermarking embedding and extraction is done for the images of different sizes. The image size 512×512 is used as the cover image. One level DWT is applied to the images to obtain the sub-band.

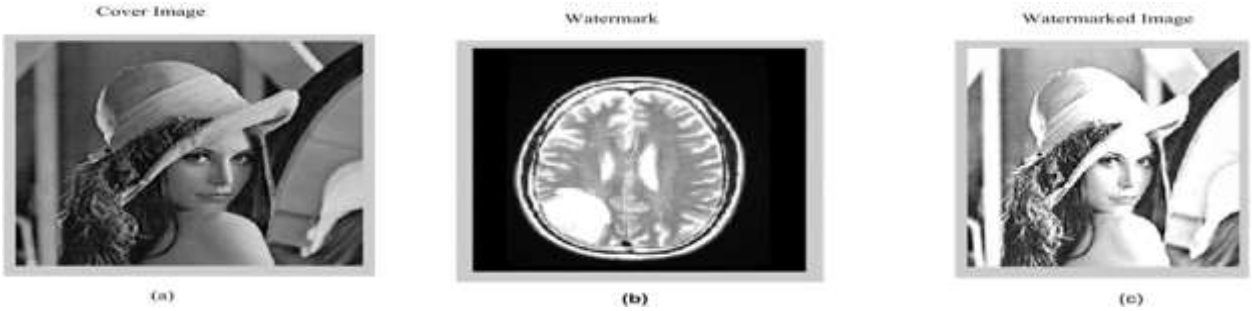

Fig. 2: (a) Cover Image **(**b). Watermark (c). Watermarked Image

TABLE1: NC Values at different gain Factors

Gain Factor	Lena	MRI-brain-tumor	MRI_head
	NC	NC	NC
0.5	0.912624	0.912624	0.912624
0.1	0.874024	0.874024	0.874024
0.05	0.861216	0.861216	0.861216
0.02	0.830708	0.830708	0.830708
0.01	0.830708	0.830708	0.830708
0.005	0.819239	0.819239	0.819239

The embedding is done to the LL sub-band by using the LSB substitution methods. The watermarked images are encrypted with RC4 encryption technique, which provide the additional security to the watermark images. We simulated our proposed algorithm using MATLAB. Based on the experimental results, the Normalized Cross Correlation (NC) and Peak Signal to Noise Ratio (PSNR) values are illustrated in Tables 1-3. The Table 1

describes the NC values at different gain factors ranging from 0.005 to 0.5. It may be observed that without any noise attack, PSNR values for all the images are above 66 dB, which indicates a high imperceptibility of the watermarked images. Tables 1 and 2 illustrate the NC and PSNR values for different images at different gain factors. The obtained NC values are above 0.819239 and show the robustness of the embedded watermark. The extracted and the original watermark images are as shown in the Figure2.

TABLE II: PSNR at different gain factor

Gain Factor	Lena	MRI-brain-tumor	MRI_head
	PSNR	PSNR	PSNR
0.5	66.989667	68.540854	68.476300
0.1	67.780468	69.445400	69.313919
0.05	67.928538	69.627140	69.490127
0.02	68.288204	70.086778	69.865561
0.01	68.288204	70.086778	69.865561
0.005	68.405682	70.244338	69.994914

In Table 3, images are attacked by the noise at different noise density for salt and pepper noise at gain factors=0.1. The maximum NC values are obtained 0.912142 at noise density 0.001 with Lena image. However, the minimum NC values are obtained 0.685349 at noise density 0.02 with MRI image.

TABLE III: NC values at gain = 0.1 against salt and pepper noise

Noise Level	Lena	MRI-brain-tumor	MRI_head
	NC	NC	NC
0.001	0.912142	0.899075	0.873004
0.002	0.903781	0.890671	0.857468
0.005	0.883014	0.851669	0.817373
0.010	0.855245	0.814487	0.764562
0.020	0.804574	0.730041	0.685349

In Table 4, the performance of the proposed solution is evaluated against the different signal processing attacks. The highest NC value is obtained 0.8210 against JPEG attack with Lena image. However, minimum NC value is 0.5780 against rotation attack with the same image.

In this table, all NC values are acceptable except the rotation attack which is less than 0.7. The proposed solution provides robust watermarking for medical data protection without degradation in the quality of the image.

5. Conclusion and Future Scope

In the medical domain, after embedding the watermark, the quality of the image should remain high for the diagnostic purposes. Our proposed method provides a robust mechanism for watermarking with high invisibility. First level DWT is used for the transforming the cover and watermark images to frequency domain. We select LL band from watermark image and format it using modulus functions. The formatted watermark is embedded in the LL band of the cover image. The watermarked image, then encrypted by using the stream cipher cryptographic techniques in order to achieved two level of security which may provide a potential solution to existing telemedicine security problem of patient identity theft. We would like improve the performance, which will be reported in future communication.

TABLE IV: NC values at different signal processing attacks

Attacks	Lena	MRI-brain-tumor	MRI_head
Cropping	0.713410	0.666059	0.652286
Rotation	0.57801	0.547633	0.660975
Gaussian LPF	0.818905	0.750601	0.670656
JPEG Compression (Quality Factor = 65)	0.821044	0.802104	0.768578
Histogram Equalization	0.819204	0.762078	0.667692
Contrast Adjustment	0.819239	0.792079	0.668578

6. References

[1] Leseley R. Matheson, Stephen G. Mitchell, Tala G. Shamoon, Robert E.Tarjan and Francis Zane , "Robustness and Security of Digital Watermarks", *Financial Cryptography, in Lecture Notes in Computer Science*, Springer, vol. 1465, 1998, pp. 227-240.

[2] G. Coatrieux, L. Lecornu,Ch. Roux, B. Sankur "A Review of Image Watermarking Applications in Healthcare" *in Proc of 28th IEEE Annual International Conference Engineering in Medicine and Biology Society*, *EMBS '06*, New York, 2006 , pp. 4691-4694.

[3] Saraj P. Mohanty, "Digital Watermarking: A tutorial Review", Report, Indian Institute of Science Bangalore, India, 1999.

[4] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, "Relevance of Watermarking in Medical Imaging," *in Proc. IEEE conference on Information Technology Applications in Biomedicin*e, Arlington, USA, 2000, pp. 250-255. http://dx.doi.org/10.1109/ITAB.2000.892396

[5] Jeanne Chen, Tung-Shou Chen and Meng Wen Cheng "A new data Hiding Method in Binary Image", *in Proc. of fifth International Symposium on Multimedia Software Engineering*, Taichung, Taiwan, 2003, pp. 88-93.

[6] Cherif Moumen and Malek Benslama "Cryptography of Medical Images", *in Proc.of Progress In Electromagnetics Research Symposium, PIERS 20*12, Kuala Lumpur, March 27-30, 2012, pp. 42-48.

[7] Hui-Mei Chao, Chin-Ming Hsu, Shaou-Gang Miaou "A Data-Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records", *IEEE Transactions on Information Technology in Biomedicine*, 6(1), March 2002, pp. 46-53.
http://dx.doi.org/10.1109/4233.992161

[8] Zhang Yun-peng, Zha Zheng-jun, Liu Wei, Nie Xuan, Cao Shui-ping and Dai Wei-di "Digital Image Encryption Algorithm Based on Chaos and Improved DES" *in Proc. IEEE International Conference on Systems, Man and Cybernetics*, San Antonio ,October 11-14, 2009, pp. 474-479.

[9] Umaamaheshvari Annamalai, Thanushkodik "Medical Image Authentication With Enhanced Watermarking Techhnique Through Visual Cryptography", *Journal of Theoretical and Applied Information Technology*, vol. 57, November, 2013, pp. 484-494.

[10] D.Bouslimi, G.Coatrieux, M. Cozic and Ch. Roux "A joint Encryption/Watermarking System for verifying the Reliability of Medical Images: Application to echographic images", *Journal of Computer Methods and Programs in Biomedicine*, Elsevier, vol. 106, April 2012, pp. 47-54.
http://dx.doi.org/10.1016/j.cmpb.2011.09.015

[11] F. Cao, H.K. Huang and X.Q. Zhou "Medical image security in a HIPAA mandated PACS environment", *Computerized Medical Imaging and Graphics*, Elsevier. vol. 27, March–June 2003, pp. 185-196.
http://dx.doi.org/10.1016/S0895-6111(02)00073-3

[12] Peter Mildenberger, Macro Eichelberg, Eric Marthin "Introduction to the DICOM Standard", *European Radiology*, Springer-Verlag,, vol. 12, April 2002, pp 920-927.
http://dx.doi.org/10.1007/s003300101100

[13] Osman Rati and Antonine Rosset "Open-source Software in Medical Imaging: Development of OsiriX", *International Journal of Computer Assisted Radiology and Surgery*, Springer-Verlag,, vol. 1, 2006, pp.187-196.

http://dx.doi.org/10.1007/s11548-006-0056-2

[14] Xiaoqi Lu, Ming Zhang, Lidong Yang, Yongjie Zhao and Jing Liu "Research and Implementation of Medical Images Management System Based on DICOM Standard", *in Proceeding of International Conference on Biological and Biomedical Sciences*, 2012, pp. 140-160.

[15] Christian Rey and Jean Luc Dugelay "A survey of watermarking algorithm for image authentication", *EURASIP Journal on Applied Signal Processing*, Hindawi, vol.6, 2002, pp. 613-621.
http://dx.doi.org/10.1155/S1110865702204047

[16] J.K. Joseph, O. Ruanaidh and Thierry Pun "Rotation, scale and translation invariant spread spectrum digital image watermarking*", Journal of Signal Processing*, Elsevier, vol. 66, 1998, pp. 303-317.
http://dx.doi.org/10.1016/S0165-1684(98)00012-7

[17] Ce LI, Baosen LI, LimeiI AO,Yaling HU,Lihua and TIAN "A Watermarking method based on Hypercomplex Fourier Transform and Visual Attention", *Journal of information and computation science*, vol. 15, 2012, pp. 4485-4492.

[18] P. W.Wong "A public key watermark for image verification and authentication", *in Proc. IEEE International Conference on Image Processing*, vol. 1, 1998, pp. 455-459.

[19] A. Giokoumaki, S.pavlopoulos and D. Koutsouris "Secure and efficient health data management through multiple watermarking on medical images", *Journal of Medical and Biological Engineering and Computing*, Springer-Verlag, vol. 44, August 2006, pp. 619-631.
http://dx.doi.org/10.1007/s11517-006-0081-x

[20] Rajendra Acharya, P. Subbanna Bhat, Sathish Kumar and Lim Choo min "Transmission and storage of medical images with patient information", *Computers in Biology and Medi*cine, Elsevier, vol. 33, 2003, pp. 303-310.
http://dx.doi.org/10.1016/S0010-4825(02)00083-5

[21] Ping WahWong and NasirMemon "Secret and Public key Image Watermarking scheme for Image authentication and ownership Verification", *IEEE Transaction on Image Processing*, November 2001, pp. 1593-1601.

[22] Rajendra Acharya , U.C. Niranjan, S.S. Iyengar, N. Kannathal and Lim Choo Min "Simultaneous storage of patient information with medical images in the frequency domain", *Computer Methods and Programs in Biomedicine*, Elsevier, vol. 76, 2004, pp. 12-19.