Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Watermarking for Health Management System

Vineet Mehan*, Renu Dhir
CSE, NIT Jalandhar
India

Y.S. Brar
EE, GNE Ludhiana
India

Abstract— Watermarking advances have conveyed efficient developments in health management system. An enormous volume of medical information is to be proficiently stored, retrieved, and circulated. This has led to the amplified security threats that have to be addressed explicitly. In this paper legitimacy of the patient and reliability of the medical image is maintained while circulating images over internet. Patient details and image information are converted to message digest using Secure Hash Algorithm (SHA). Advanced Encryption Standard (AES) is then applied to generate encrypted authentication code. Generated code is implanted using Discrete Cosine Transform (DCT) methodology. Embedding of authentication code certifies image veracity with respect to a specific patient. Analysis of quantitative parameters reveals the effectiveness of the proposed approach.

Keywords— Watermarking, SHA, AES, DCT, Image Authentication.

I. INTRODUCTION

Health apprehensions are the most important rudiments of human being. One of the chief liberties of all human beings is the enchantment for upright health. With the involvement of digital expertise in the arena of medical imaging, there has been culmination in the healthcare [1]. The replacement of scrambled paper documents with the digital counterparts has directed to proficient organization of electronic patient record [2]-[4]. Numerous images are distributed over Internet to far placed doctors for telediagnosis [5]. The support of technology rose associated menaces with shared electronic patient records. It is necessary to take description of the aspects such as authentication and reliability with the sharing of images in the Health Management System [6]. Watermarking techniques offers several striking features for the healthcare business [7]-[9]. It amends the image information invisibly to implant the watermark. Watermark might encompass the patient medical information along with doctor's distinctiveness. Irrespective of the assistances, the watermarking method may come across environs in medical images. The implanted watermark signal often amends the cover image in an irreversible mode and could disguise subtle information. The proposed system endeavours to maintain the image diagnosis eminence without vital information loss. This paper deliberates the apprehensions regarding legitimacy and reliability of digital medical images related to patients for competent telediagnosis and teleconsulation purpose. This paper is structured as follows. Literature Review related with stated research work is detailed in Section II. Key components are indicated in Section III. Experimental Results are given in Section IV. Finally the concluding notes are listed in Section V.

II. LITERATURE REVIEW

To maintain authenticity and integrity of digital mammography images Zhou et al. [10] proposed an efficient technique. Four modules identified for the proposed approach include: Image pre-processing, image hashing, data encryption and data embedding. In the pre-processing section breast pixels are mined from the background pixels. In this step patient information is also recovered from the image header. Hash value of the mammogram image is computed using Message Digest Algorithm (MDA-MD5). Message digest of 128 bit is generated. Digest acts as an input to create digital signature using RSA. Signature is integrated with patient information and encrypted using Data Encryption Standard (DES) with 56 bit key. The encrypted data is embedded in the image using Least Significant Bit (LSB) technique. Data integrity is verified by matching the decrypted hash value retrieved from the image. A digital watermarking scheme for copyright protection of images is given by Samuel and Penzhorn [11]. Watermark is encrypted using Advanced Encryption Standard (AES). Encrypted content is then hashed by means of Secure Hash Algorithm (SHA-1). Message digest of 160 bit is generated to check if any kind of tampering has been done or not. Watermark is embedded by exploiting the DCT coefficients. Experimental results show acceptable degradation level while maintaining the quality of the image. PSNR of 35 dB and above infers for the adequate degradation levels.

Giakoumaki et al. [12] presented multiple watermarking for Health Information System (HIS). In this paper multiple watermarks are implanted into the medical images. Watermarks carry patient's particulars, diagnostic information, doctor's digital signature for certification, and a reference note for data reliability. Watermarks are inserted into four decomposition levels using wavelet coefficients. Kobayashi et al. [13] presented a novel technique by means of cryptography to enhance reliability of medical images. The technique delivers a stronger association concerning image and data on its integrity and legitimacy without negotiating on quality of image. Data is encrypted using AES with 256 bits key length. Secure hash standard specified by NIST [14] is used to generate a condensed representation of the message. SHA-512/224 and SHA-512/256 are the two truncated additions made to the previous standards.

III. KEY COMPONENTS

A. Watermarking in Medical Imaging

Digital watermarking is smeared in the e-health setting for teleconsulation and telediagnosis tenacity [15]-[16]. Medical images incorporate diagnostic data which can be used for timely recognition of the diseases. It is beneficial to maintain patient information, content authorization and medical image consistency [17]. Images are watermarked to prove the integrity by confirming that the image was not altered by illicit person [18]. Watermarking is also applied to determine the authenticity by confirming that the image belongs to the right patient and exact source. Processing domain splits the watermarking arrangement into two groups [19]-[21]: Spatial domain watermarking and Frequency domain watermarking. Spatial domain watermarking alters the image pixels directly based on the watermark that has to be inserted. Frequency domain watermarking applies the transformation and embeds the watermark into the frequency coefficients. The major limitation with watermarking is visual artifacts familiarized by data implanting. The accuracy of diagnosis and cure of patients considerably is subjected on the received watermarked image by clinician. Distorted image often obstructs correct diagnosis, cure and can lead to risk of life [22]. To avert the specified limitations a frequency domain method of watermarking is proposed by this research work.

B. Image Authentication

Fragile watermarking ensures true image authentication by detecting any king of tampering done to the medical images. Authentication is the protection of the cooperating associations, counter to the attacks by a third party. A threat arises when the associations are suspicious and try to achieve negation. Secure Hash Algorithm endows identification of the message integrity [23]-[25]. The algorithm outcomes completely different message digests by altering a single bit change in the original message. SHA is demarcated in two stages: pre-processing and hash computation [26]. The pre-processing stage involves pre-processing the message, parsing the message and then setting the initial hash value. The hash computation generates an authentication code by applying functions, constants and word operations iteratively to create a series of hash values. Computing the hash values generates the final message digest. Further, encryption is prepared to make the information unreachable to illicit persons. AES is applied to create an encrypted output.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A set of 25 medical images of 512x512 dimensions are taken for the experimental purpose. Implanted watermark entail details of patient with fields which consist of Patient Identification Number (PID), Patient Name (ON), Patient Address (PA), Patient Clinical Details (PCD), Patient Diagnosis (PD) and Doctor's Name (DN). Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) quality parameters are calculated for each image with varying watermark size in range of 256-3328. Insertion Time (IT) and Extraction Time (ET) are estimated to conclude the processing time while inserting and retrieving of watermark. IT and ET are calculated in milliseconds (ms).

TABLE I
QUANTATIVE PARAMETER ANALYSIS OF MEDICAL IMAGES

S.No.	Image Name	Watermark Size (bits)	PSNR (R)	PSNR (G)	PSNR (B)	MSE	MPSNR	IT (ms)	ET (ms)
1	Image1	256	66.39	69.21	77.68	0.0079	69.15	234	109
2	Image2	384	66.44	66.93	67.12	0.0135	66.83	234	109
3	Image3	512	64.26	64.93	66.06	0.0205	65.01	249	109
4	Image4	640	61.97	62.96	63.76	0.0339	62.83	265	109
5	Image5	768	65.86	62.34	62.26	0.0312	63.19	265	109
6	Image6	896	61.67	61.8	61.75	0.0436	61.74	280	93
7	Image7	1024	61.5	61.07	60.95	0.0497	61.17	280	109
8	Image8	1152	63.21	60.48	60.34	0.0498	61.16	327	124
9	Image9	1280	64.94	58.99	58.95	0.0619	60.21	296	124
10	Image10	1408	60.21	60.35	60.63	0.0594	60.39	343	124
11	Image11	1536	61.22	59.07	58.74	0.0722	59.55	343	156
12	Image12	1664	57.28	57.32	58.59	0.1106	57.69	312	109
13	Image13	1792	61.76	58.22	57.86	0.0826	58.96	296	93
14	Image14	1920	58.06	55.64	55.66	0.1519	56.32	343	107
15	Image15	2048	58.54	59.07	59.17	0.0835	58.91	343	109
16	Image16	2176	54.47	54.55	68.45	0.1564	56.19	358	109
17	Image17	2304	57.21	57.63	57.99	0.1131	57.6	390	124
18	Image18	2432	74.26	55.99	55.92	0.1109	57.68	327	93
19	Image19	2560	58.39	57.34	57.42	0.1105	57.7	327	109
20	Image20	2688	58.42	57.94	58.11	0.0995	58.15	327	109
21	Image21	2816	56.75	57.26	57.45	0.1256	57.14	343	109
22	Image22	2944	56.61	56.83	56.62	0.1394	56.69	327	93
23	Image23	3072	57.07	56.71	56.5	0.1374	56.75	349	105
24	Image24	3200	55.79	54.77	54.73	0.2024	55.07	375	108
25	Image25	3328	58.08	56.68	56.29	0.1312	56.95	468	135

Minimum (M_N) and maximum (M_X) parameter values obtained are shown in Table II. Average value (A_G) of parameters using complete set of test images is displayed in Table III.

TABLE II
M_N AND M_X PARAMETER VALUES

PSNR(R)		PSNR(G)		PSNR(B)		MSE		MPSNR		IT		ET	
M_N	M_X	M_N	M_X	M_N	M_X	M_N	M_X	M_N	M_X	M_N	M_X	M_N	M_X
54.47	74.26	54.55	69.21	54.73	77.68	0.0079	0.20240	55.07	69.15	234	468	93	156

TABLE III
A_G PARAMETER VALUES

A_G PSNR(R)	A_G PSNR(G)	A_G PSNR(B)	A_G MSE	A_G MPSNR	A_G IT	A_G ET
60.81	59.36	60.36	0.0879	59.72	320.04	111.48

Comparative analysis of PSNR for R, G, B and MPSNR w.r.t. varying watermark size is presented in Fig. 1. Comparative analysis of EPT and RPT for each test image is displayed in Fig. 2.

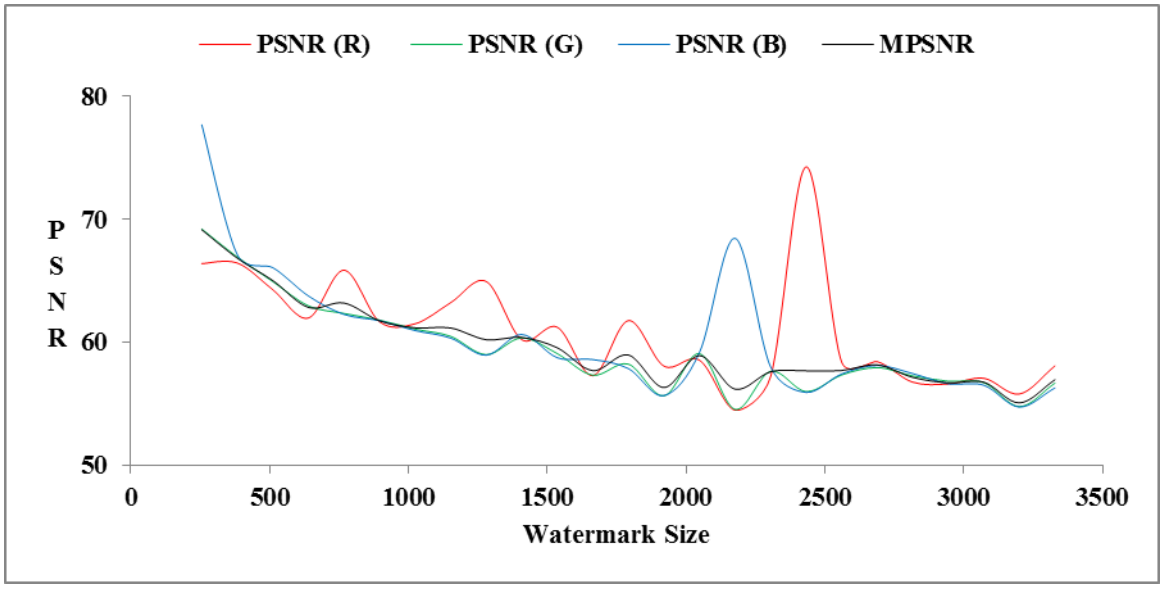

Fig. 1 Comparisons of R, G, B and MPSNR w.r.t. varying watermark size.

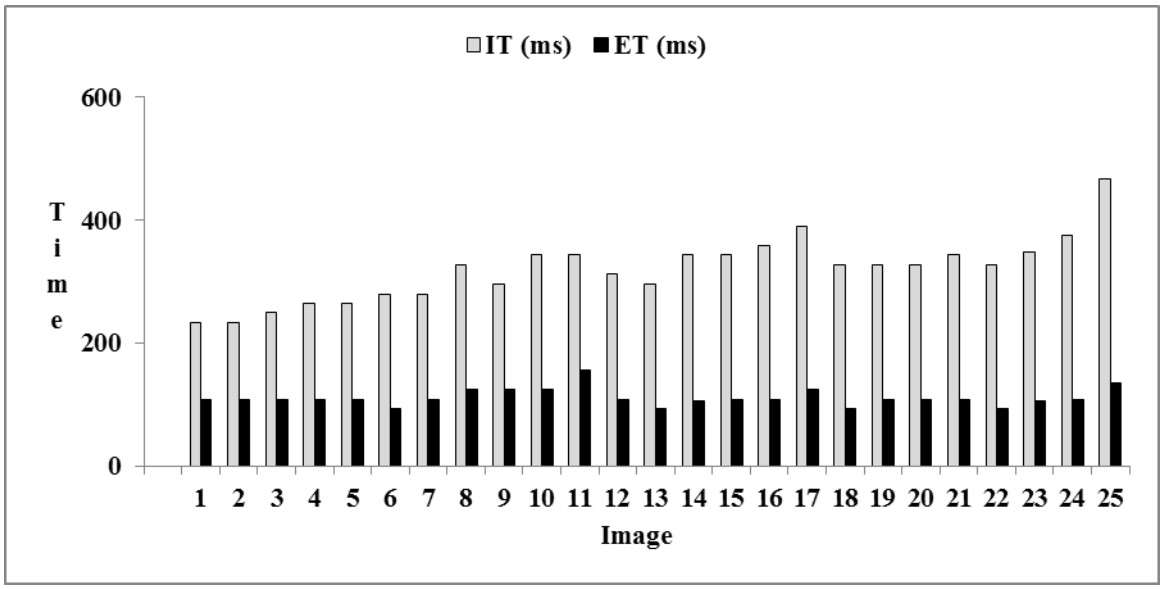

Fig. 1 IT and ET comparisons for medical images.

V. CONCLUSIONS

In this paper an image certification, integrity confirmation and organization of the patient records structure is presented. The work is chiefly applied in the realm of colored digital image. The encrypted authentication code is generated using SHA and AES. The hash function conveys additional security sustenance. The proposed watermarking technique reports necessary concerns by invisibly inserting watermarks into the frequency coefficients of medical images.

The investigational outcomes establish the effectiveness of the system. Results ascertain that the recommended system provides virtuous visual quality of the watermarked image which can aid in the medical diagnosis effectually.

REFERENCES

[1] A. Berler, S. Pavlopoulos, and D. Koutsouris, "Using key performance indicators as knowledge-management tools at a regional health-care authority level ," *IEEE Transactions on Information Technology in Biomedicine*, vol. 9 , no. 2, pp. 184-192, Jun. 2005.

[2] H.-M. Chao, C.-M. Hsu, and S.-G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 6, no. 1, pp. 46-53, Mar. 2002.

[3] G. H. M. B. Motta and S. S. Furuie, "A contextual role-based access control authorization model for electronic patient record," *IEEE Transactions on Information Technology in Biomedicine*, vol. 7 , no. 3, pp. 202-207, Sep. 2003 .

[4] D. C. Leonard, A. P. Pons, and S. S. Asfour, "Realization of a Universal Patient Identifier for Electronic Medical Records Through Biometric Technology ," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 4, pp. 494-500, Jul. 2009.

[5] G. Coatrieux, C. Le Guillou, J. .-M. Cauvin, and C. Roux, "Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 2, pp. 158-165, Mar. 2009.

[6] M. Wang, C. Lau, F. A.,. I. Matsen, and Y. Kim, "Personal health information management system and its application in referral management," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 3, pp. 287-297, Sep. 2004.

[7] H. K. Lee, H. J. Kim, K. R. Kwon, and J. K. Lee, "Digital watermarking of medical image using ROI information," in *Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry*, 2005, pp. 404-407.

[8] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management ," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.

[9] Bouslimi, D., G. Coatrieux, M. Cozic, and C. Roux (2012) "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 5, pp. 891-899. Zhou, X. Q., H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," IEEE Transactions on Medical Imaging, Vol. 20, No. 8, 2001, pp. 784-791.

[10] Samuel, S., and W. T. Penzhorn, "Digital watermarking for copyright protection," *7th AFRICON Conference* in Africa, 2004, pp. 953-957.

[11] Giakoumaki, A., S. Pavlopoulos, and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 10, No. 4, 2006, pp. 722-732.

[12] Kobayashi, L. O. M., S. S. Furuie, and P. S. L. M. Barreto (2009) "Providing Integrity and Authenticity in DICOM Images: A Novel Approach," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 13, No. 4, pp. 582-589.

[13] NIST, "Secure Hash Standard (SHS)," *Federal Information Processing Standards*, No. 180-4, 2012, pp. 1-30.

[14] S. Cheng, Q. Wu, and K. R. Castleman, "Non-ubiquitous digital watermarking for record indexing and integrity protection of medical images," in *IEEE International Conference on Image Processing*, 2005 , pp. 1062-1065.

[15] V. Fotopoulos, M. L. Stavrinou, and A. N. Skodras, "Medical image authentication and self-correction through an adaptive reversible watermarking technique ," in *8th IEEE International Conference on BioInformatics and BioEngineering*, 2008 , pp. 1-5.

[16] L.-Q. Kuang, Y. Zhang, and X. Han, "A Medical Image Authentication System Based on Reversible Digital Watermarking," in 1st *International Conference on Information Science and Engineering (ICISE)*, 2009 , pp. 1047-1050.

[17] Y. M. Cheung and H. T. Wu, "A Sequential Quantization Strategy for Data Embedding and Integrity Verification," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 8, pp. 1007-1016, Aug. 2007 .

[18] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE*, vol. 90, no. 1, pp. 64-77, Jan. 2002.

[19] S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 154-165, Feb. 2004.

[20] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 906-924, Apr. 2003.

[21] R. F. Olanrewaju, O. Khalifa, A. Abdulla, and A. M. Z. Khedher, "Detection of alterations in watermarked medical images using Fast Fourier Transform and Complex-Valued Neural Network," in *4th International Conference On Mechatronics*, 2011, pp. 1-6.

[22] C. H. Lin, C. Y. Lee, Y. S. Yeh, H. S. Chien, and S. P. Chien, "Generalized secure hash algorithm: SHA-X," in *IEEE International Conference on Computer as a Tool*, 2011, pp. 1-4.

[23] J. Docherty and A. Koelmans, "A flexible hardware implementation of SHA-1 and SHA-2 Hash Functions," in *IEEE International Symposium on Circuits and Systems* , 2011 , pp. 1932-1935.

[24] S. Gueron, "Speeding Up SHA-1, SHA-256 and SHA-512 on the 2nd Generation Intel® Core™ Processors," in *Ninth International Conference on Information Technology: New Generations*, 2012, pp. 824-826.

[25] National Institute of Standards and Technology, "Secure Hash Standard," *Federal Information Processing Standards Publication* 180-4, 2012.

[26] X. Jian and M. Bin, "Digital watermark for document electronic seal system based on DCT technology," in *International Conference on Uncertainty Reasoning and Knowledge Engineering*, 2011, pp. 5-8.

[27] D. Teng, R. Shi and X. Zhao, "DCT Image Watermarking Technique Based on Mix of Time Domain," in IEEE *International Conference on Information Theory and Information Security*, 2010 pp. 826-830.

[28] Z. Li, Z. P. Ping, Q. G. Bin and J. Zhen, "Image Watermarking with optimum capacity," in *5th International Conference on Visual Information Engineering*, 2008 pp.117-123.

[29] V. M. Potdar, S. Han and E. Chang, "A Survey of digital watermarking techniques," *3rd IEEE Conference on Industrial Informatics*, 2005 pp.709-716.

