Extraction and Authentication of Hidden Patient's Information from Biomedical Image through Crypto-Watermarking Technique

Subhajit Koley
Electronics & Communication Engineering,
Guru Nanak Institute of Technology
Kolkata, India
subhajitgnitece@gmail.com

Koushik Pal
Institute of Radio Physics and Electronics,
University of Calcutta
Kolkata, India
koushik.rpe@gmail.com

Goutam Ghosh
Institute of Radio Physics and Electronics,
University of Calcutta
Kolkata, India
goggle.rpe@gmail.com

Mahua Bhattacharya
Indian Institute of Information
Technology and Management,
Gwalior, India
mahuabhatta@gmail.com

***Abstract*— This paper describes a new biomedical image Crypto-Watermarking technique in the spatial domain by which Electronic Patient's Record, Doctor's Signature and Diagnostic Center Logo can be hidden in both gray-scale and colour images to ensure greater security, accurate recovery and data authenticity. The proposed method is a combination of RSA algorithm of cryptography and LSB replacement watermarking technique. The EPR is converted into cipher text data using public - private key with the help of RSA encryption method and the cipher text data is embedded into cover image using LSB replacement. In the detection process, watermark is detected from LSB of the watermarked image. Then the watermark or the cipher text is converted into plaintext using RSA decryption technique. Security is achieved in the proposed crypto-watermarking by the inclusion of keys embedded in the cover image. Experimental results show improvement in both the visual and statistical invisibility of the hidden information. The recovered information is also same as hidden one which is also supported by several image quality metrics.**

Keywords- Biomedical image; spatial domain watermarking; cryptography; Crypto-Watermarking; LSB; image quality metrics

I. INTRODUCTION

Nowadays transmission and storage of medical images in digital form has increased rapidly in biomedical field through the internet. The necessity of fast and secure diagnosis is vital in the medical world. It makes possible for physicians from different areas to serve a patient. The patient can obtain the possible best service from this medical process while maintaining their integrity and confidentiality against the attacks of unauthorized pirates and hackers [1].

A. Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks like the Internet so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptanalysts are also called attackers [2, 3].

B. Watermarking

Watermarking is the process of embedding a message on a host signal. Watermarks may be used to verify the authenticity or integrity of the recover data or to show the identity of its owners. Digital Watermarking can be done using software or hardware. But the efficiency of the watermarking technique is found out with the capacity, robustness and perceptibility of the method [4].

C. Cryptography and watermarking tackles the same issue: data security. In cryptography, the message is hidden in the cipher but an interception of the message can be damaging, as it still shows that there is communication between the sender and receiver. In contrast, Watermarking takes a different approach in hiding the evidence that even a communication is taking place. However, cryptography provides no protection once the content is decrypted, which is required for human perception. Watermarking complements cryptography by embedding a message within the content. If properly designed, the message remains in the content after decryption and, more importantly, after digital-to-analog and analog-to-digital conversion [5].

ISBN: 978-81-923777-9-7

D. Crypto-Watermarking

Crypto-Watermarking technique is a combination of cryptography and watermarking methodology. Digital representation of signals brings many advantages such as lossless copying, convenient distribution over networks, easy editing and modification. Unfortunately, these advantages bring in serious problems such as widespread copyright violation and illegal copying, and distribution.

Cryptography is used to convert the plain text into cipher text to protect the information. A popular algorithm in cryptography is RSA. It's a public key cryptography that is based on the presumed difficulty of factoring large integers. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publically described the algorithm in 1977. The RSA algorithm involves three steps: key generation, encryption and decryption. But cryptographic techniques do not completely solve the problem of unauthorized copying.

Digital watermarking is a technology being developed to provide protection from illegal copying. It involves embedding information into a digital image such that, if the image is copied, then the information is also carried into the copy. Typically, the information is a diagnostic center logo or a patient's record which identifies the owner of the image. Thus, watermarking can be used to identify the content owner and medical result detected after the image has been modified but not destroyed beyond recognition [6, 7].

E. Requirements and Relevance of Digital Watermarking in Biomedical field

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible.

Biomedical image watermarking is a relevant process for enhancing data security, content verification and image fidelity. Embedding external data in medical images should not change any information, thereby affecting further applications. Biomedical image watermarking embeds messages imperceptibly without changing image size or format [8]. Protection of EPR (Electronic Patient Record) in digital health care system is very important. Hiding patient data as EPR in the medical image is one of the applications of digital image watermarking [9, 10].

II. Proposed Methodology

A. Embedding

A biomedical gray-scale or colour image is taken as cover image. Then the cover image is split into four parts: upper left, upper right, lower left, lower right. Then upper left part and lower right part are taken and the RGB is converted into YCbCr colour space and colour components Y, Cb, Cr are extracted from YCbCr colour space image. The patient's name and the doctor's name are taken as a patient's record and it is converted into its ASCII value and it is flipped. Then 2 prime no's are taken to generate public key and private key.

The patient's name and the doctor's name (plain text) are converted into the cipher text using RSA algorithm encryption method. The cipher text is embedded into Cb, Cr components using LSB replacement method. Then the lower left part of the cover image is taken and the RGB is converted to YCbCr colour space and extracted colour components Y, Cb, Cr. The doctor's signature and the diagnose center logo are taken and embedded into Y components of lower left part of the cover image. Then the keys are embedded into the upper right part of the cover image. Once the data has been embedded, the 4 parts of the image are joined and hence the watermarked image is created.

Flowchart of the embedding technique is given in details in Fig.1.

B. Recovery

The watermarked image is taken as the input and it is split into four parts: upper left, upper right, lower left, lower right. The upper right part is taken and the RGB is converted into YCbCr colour space and the colour components Y, Cb, Cr are extracted from YCbCr colour space image. Using counter, the watermark values are decided from the watermarked image and recovered the keys. Similarly, watermark of the patient's records are decoded from upper left and lower right part of the watermarked image. Using keys, watermark (cipher text) is converted into plain text with the help of RSA algorithm decryption method and it is flipped. Then the doctor's signature and the diagnosis center logo are found out from LSB of the lower left part of the watermarked image. Once the data has been decoded, the 4 parts of the image are joined together. Thus, we recover the original biomedical image and also various hidden information.

III. Results & Discussions

In table 1, four sets of gray-scale biomedical cover images and in table 2, four sets of colour biomedical images along with patient information, doctor's signature and diagnose center logo and obtained watermarked images are shown as the outcome of our proposed methodology. The calculated

ISBN: 978-81-923777-9-7

value of the quality metrics such as PSNR and SSIM, SC, NCC, BER, UIQI are also given to find the image quality. Higher value of PSNR, SSIM, NCC, and UIQI represents image of good quality while lower values of BER, SC represent less error and consequently good quality image [11, 12]. It is observed that the difference between the watermarked image and the cover image by the Human Visual System appear to be identical. From table 1 and table 2, we observe that the PSNR value is quite higher which indicates good quality of picture. The value of SSIM in all the cases is close to 1 which describes a good structural similarity between the original and watermarked image and BER is close to 0 which indicates less error in watermarked image. The value of NCC and UIQI are also close to 1 which is proof of the good quality of the watermarked image.

From table 1 and table 2, we can also see that patient information, doctor's signature and diagnose center logo are successfully recovered from the watermarked images. Doctor's signature and diagnostic center logo are visually and statistically similar to the original signatures and logos that have been hidden. The values of SSIM and NCC are very close to 1 and the values of BER are close to 0. The values of NCC prove the quality of the recovered watermark or information signature and logo and lower values of BER represent less error. It is clear that the proposed methodology is very much good to hide patient's information and as well as for logo and strong enough to reconstruct legible information from the watermarked image for both black & white and colour biomedical images.

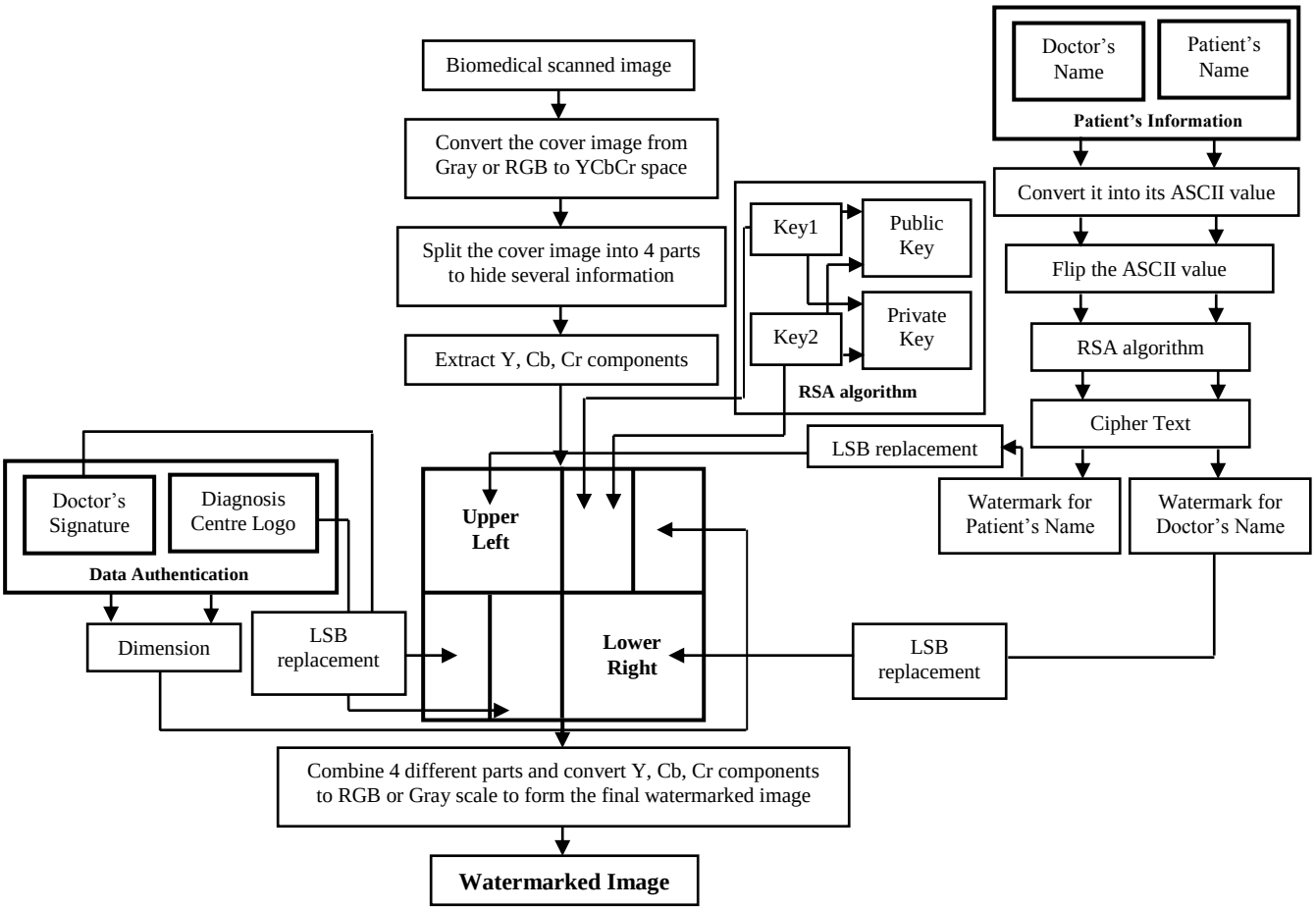
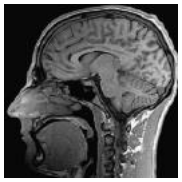
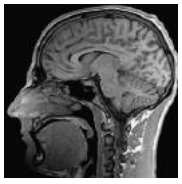
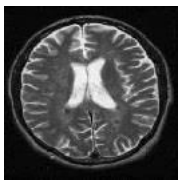
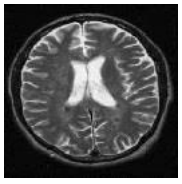
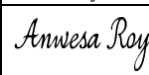
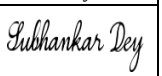
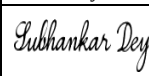


Fig1: Flowchart of the proposed Crypto-Watermarking Embedding Technique

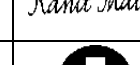
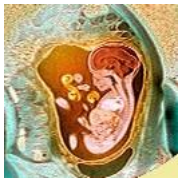
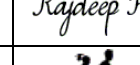
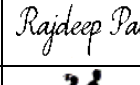
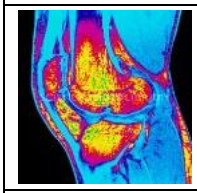
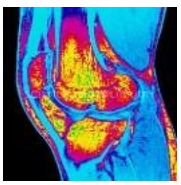
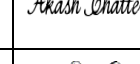
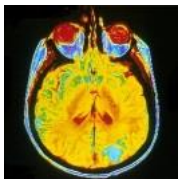
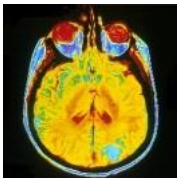
ISBN: 978-81-923777-9-7

TABLE 1: EXPERIMENTAL RESULTS FOR GRAY-SCALE IMAGES AND IMAGE QUALITY METRICS

Biomedical Cover Image	Data to be Hidden		Watermarked Image	Image Quality Metrics for Watermarked Image		Recovered Data		Image Quality Metrics for Recovered Signature and Logo	
	Patient's Record					Patient's Record			
 Hand X Ray	**Name**	Partho Bag		PSNR	56.921	**Name**	Partho Bag		
	Doctor's Name	Dr. Animesh Laha		BER	0.132	**Doctor's Name**	Dr. Animesh Laha		
	Doctor's Signature			SC	0.999	**Doctor's Signature**		SSIM	1
				SSIM	0.999			NCC	1
								BER	0
	Diagnostic Centre logo					**Diagnostic Centre logo**		SSIM	1
				NCC	1.000			NCC	1
				UIQI	0.993			BER	0
 Head MRI	**Name**	Gaurav Das		PSNR	57.888	**Name**	Gaurav Das		
	Doctor's Name	Dr. Rahul Debnath		BER	0.105	**Doctor's Name**	Dr. Rahul Debnath		
				SC	0.998				
	Doctor's Signature			SSIM	0.999	**Doctor's Signature**		SSIM	1
								NCC	1
				NCC	1.000			BER	0
	Diagnostic Centre logo					**Diagnostic Centre logo**		SSIM	1
				UIQI	0.999			NCC	1
								BER	0
 Brain MRI	**Name**	Mayuri Dey		PSNR	56.265	**Name**	Mayuri Dey		
	Doctor's Name	Dr. Anwesa Roy		BER	0.153	**Doctor's Name**	Dr. Anwesa Roy		
				SC	0.998				
	Doctor's Signature			SSIM	0.999	**Doctor's Signature**		SSIM	1
								NCC	1
								BER	0
	Diagnostic Centre logo			NCC	1.000	**Diagnostic Centre logo**		SSIM	1
								NCC	1
				UIQI	0.996			BER	0
 Knee MRI	**Name**	Pinaki Roy		PSNR	55.551	**Name**	Pinaki Roy		
	Doctor's Name	Dr. Subhankar Dey		BER	0.181	**Doctor's Name**	Dr. Subhankar Dey		
	Doctor's Signature			SC	0.997	**Doctor's Signature**		SSIM	1
				SSIM	0.994			NCC	1
								BER	0
	Diagnostic Centre logo			NCC	1.001	**Diagnostic Centre logo**		SSIM	1
								NCC	1
				UIQI	0.925			BER	0

ISBN: 978-81-923777-9-7

TABLE 2: EXPERIMENTAL RESULTS FOR COLOUR IMAGES AND IMAGE QUALITY METRICS

Biomedical Cover Image	Data to be Hidden: Patient's Record		Watermarked Image	Image Quality Metrics for Watermarked Image		Recovered Data: Patient's Record		Image Quality Metrics for Recovered Signature and Logo	
 Head MRI	**Name**	Bishal Dey		PSNR	52.599	**Name**	Bishal Dey		
	Doctor's Name	Dr. Ranit Maity		BER	0.310	**Doctor's Name**	Dr. Ranit Maity		
	Doctor's Signature			SC	0.999	**Doctor's Signature**		SSIM	1
				SSIM	0.998			NCC	1
								BER	0
	Diagnostic Centre logo			NCC	1.000	**Diagnostic Centre logo**		SSIM	1
				UIQI	0.994			NCC	1
								BER	0
 Foetus MRI	**Name**	Anindita Basak		PSNR	52.520	**Name**	Anindita Basak		
	Doctor's Name	Dr. Rajdeep Pal		BER	0.322	**Doctor's Name**	Dr. Rajdeep Pal		
				SC	0.999				
	Doctor's Signature			SSIM	0.999	**Doctor's Signature**		SSIM	1
								NCC	1
								BER	0
	Diagnostic Centre logo			NCC	1.000	**Diagnostic Centre logo**		SSIM	1
				UIQI	0.998			NCC	1
								BER	0
 Knee MRI	**Name**	Susmit Saha		PSNR	52.703	**Name**	Susmit Saha		
	Doctor's Name	Dr. Akash Chatterjee		BER	0.327	**Doctor's Name**	Dr. Akash Chatterjee		
				SC	0.999				
	Doctor's Signature					**Doctor's Signature**		SSIM	1
				SSIM	0.995			NCC	1
								BER	0
	Diagnostic Centre logo			NCC	1.000	**Diagnostic Centre logo**		SSIM	1
								NCC	1
				UIQI	0.908			BER	0
 Brain MRI	**Name**	Souvick Laha		PSNR	53.025	**Name**	Souvick Laha		
	Doctor's Name	Dr. Girish Ghosh		BER	0.293	**Doctor's Name**	Dr. Girish Ghosh		
	Doctor's Signature			SC	0.999	**Doctor's Signature**		SSIM	1
				SSIM	0.996			NCC	1
								BER	0
	Diagnostic Centre logo			NCC	1.000	**Diagnostic Centre logo**		SSIM	1
								NCC	1
				UIQI	0.968			BER	0

ISBN: 978-81-923777-9-7

IV. CONCLUSION

It is a need of healthcare industry to transmit biomedical images from one geographical location to other using internet. Improvement in information and communication technologies made it possible to handle such applications through electronics component. But security is essential factor. Security level should be high and producing exact recovery of original watermark for standard image database. The proposed biomedical image Crypto-Watermarking scheme in the spatial domain includes procedures for data embedding, extraction and verification of quality for both watermarked image and the recovered watermark. We observed that the original patient information, doctor's signature and diagnostic center logo can be recovered exactly by the proposed algorithm at the receiver end.

The image quality metrics support the quality, strength and satisfy the high performance of the proposed algorithm. The results obtained show satisfying statistics of the performance of the proposed algorithm. The Crypto-Watermarking algorithm technique is very much efficient and a newer approach which is very unique and easy to understand. Hence we can conclude by stating the fact that the proposed algorithm provides a method for secure communication and data hiding for both gray-scale image and colour biomedical images in modern health care system.

REFERENCES

[1] J. Nayak, P Subbanna Bhat, R. Acharya and Niranjan; "Simultaneous storage of medical images in the spatial and frequency domain: a comparative study"; BioMedical Engineering OnLine 2004, pp:3-17.

[2] G. N. Swamy, K. S. Rao, A. R. Kumar; "A watermarking technique based on visual cryptography"; Journal of Information Assurance and Security 4, 2009, pp:470-473.

[3] Behrouz A. Forouzan, Data Communications and Networking, 4/e, McGraw-Hill Higher Education, ISBN: 0072967757, 2007

[4] I. J. Cox, M. Miller, J. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers, 2002.

[5] J. Dittmann, P. Wohlmacher, Klara Nahrstedt; "Multimedia and security using cryptographic and watermarking algorithm" ieee multimedia © 2001 ieee

[6] B. Smithal and K.A. Navas "Spatial Domain- High Capacity Data Hiding in ROI Images" IEEE - ICSCN 2007.

[7] Mohamed Ali HAJJAJI, E. BOURENNANE; "Watermarking of medical image: method based "lsb""; VOL.2, NO. 12, ISSN 2079-8407, Journal of Emerging Trends in Computing and Information Sciences, December 2011.

[8] K. Pal, G. Ghosh, M. Bhattacharya, "Retrieval of Hidden Infected Region using Biomedical Image Watermarking for Tele-diagnosis to Ensure Better Treatment", IEEE International Conference on Computers & Devices for Communication, Kolkata, 17-19 December 2012.

[9] A. Umaamaheshvari, K. Thanushkodi; "High performance and effective watermarking scheme for medical images" ; European Journal of Scientific Research,ISSN 1450-216X Vol.67 No.2 2012,pp:283-293.

[10] K. Pal, G. Ghosh, M. Bhattacharya, "Reversible Digital Image Watermarking using Bit Replacement and Majority Algorithm Technique", Journal of Intelligent Learning Systems and Applications, ISSN: 2150-8402, Scientific Research Incorporation group, USA, Vol 4, Number-3, August 2012, pp.199-206.

[11] T. Lehmann, A. Sovakar, W. Schmitt, R. Repges, "A comparison of similarity measures for digital subtraction radiography''. Comput. Biol. Med. 27, 1997, pp:151–167.

[12] M. Eskicioglu and P. S. Fisher, "Image Quality Measures and Their Performance," IEEE Transactions on Communications, vol. 43, no. 12, December 1995, pp. 2959-2965.

ISBN: 978-81-923777-9-7