International Journal of Pure and Applied Mathematics
Volume 118 No. 8 2018, 265-269
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Combined Cryptography And Digital watermarking For Secure Transmission of Medical Images in EHR Systems

Pooja Prakash.M
Department of Computer Science and Engineering
Royal College of Engineering and Technology
Thrissur, Kerala, India
poojaprakash995@gmail.com

Sreeraj.R
Department of Computer Science and Engineering
Royal College of Engineering and Technology
Thrissur, Kerala, India
sreerajr@royalcet.ac.in

Fepslin AthishMon
Department of Computer Science and Engineering
Royal College of Engineering and Technology
Thrissur, Kerala, India
fepslin@gmail.com

K. Suthendran
Department of Information Technology
Kalasalingam Academy of Research and Education
Krishnankoil,India
k.suthendran@klu.ac.in

***Abstract*—Telemedicine uses telecommunication and information technology is uesd to provide clinical health care from distance. The information privacy and security issues continue to plague telemedicine, especially due to the extensive use of new communication technologies like wireless network in today's world. Medical images contain very sensitive information, which should not be made accessible to unauthorized persons. so, in order to protect patient privacy, integrity and confidentiality. By using encryption and digital watermarking we can provide the confidentiality, authenticity and to the medical images. In this paper, we combine the cryptography and digital watermarking techniques for medical image transmission. DWT and DCT combination is used for the watermarking technique and ECDH (Elliptical Curve Diffie Helman) algorithm is used for cryptographic technique**

Keywords*— *Cryptograph; Medical image; Digital watermarking; DWT; DCT; ECDH

I. INTRODUCTION

Nowadays medical image sharing through internet becomes very popular to make clinical health care from distances. When sharing the medical images with patient data we should provide high security i.e. Integrity, Authentication, Confidentiality to the contents presents in the medical image .In this paper we discuss different method for medical image security. By using encryption and digital watermarking we can provide the confidentiality, authenticity and to the medical images. In this paper, we combine the cryptography and digital watermarking techniques for medical image transmission. DWT and DCT combination is used for the watermarking technique and ECDH (Elliptical Curve Diffie Helman) algorithm is used for cryptographic technique.

Watermarking is used to hiding the information such as hide secret information in digital media like photographs, digital music, or digital video. Nowadays which has seen a lot of research images are need to be stored for future reference. For medical image security, when the image is interest. The Medical images are also much important in the field of medicine, all these medical acquired the physician embeds watermarks into the medical image before storing. Any authorized member of the healthcare personal, having the appropriate key, can extract the embedded watermarks and gain access to information.

Encryption techniques used to provide security to data. In encryption, the information is encoding to prevent unauthorized access and the unauthorized persons cannot read it. The encryption process, the information is encrypted using an encryption algorithm, with the help of key. Also data can be embedded within the image for secure transmission become more secure, in which data embedded by using data hiding algorithm with the help of key. Image transmission among clinicians through insecure Internet is one of the most important applications of medical image encryption. We can use an encryption scheme for encrypt medical image then only the authorized person can decrypt this medical image and can obtain the original image. The ownership of these medical images is very important to improve.

In this paper, we combine the cryptographic and digital watermarking techniques for the secure transmission of medical image over the internet. Here the combination of DWT and DCT algorithm is used for watermarking technique. And the ECDH algorithm is used for cryptographic method and here the integrity of received image is also calculated.

In section II we will discuss the literature survey. Then in section III we describes the proposed method. In the section IV we discuss results and screenshot of this method and finally section V include the conclusion.

II. Literature Review

Sudip Ghosh, Sayandip De, Santi Prasad Maity, Hafizur Rahaman [1] published in International Conference on Electrical Information and Communication Technology (EICT 2015) "A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and cryptography Using Extended Hamming Code". In this paper they proposed a dual purpose spatial domain robust algorithm for image cryptography and digital image watermarking .Where a key is generated using 'Extended Hamming Code' to make the code self-correcting. The proposed cryptographic algorithm is applicable for symmetric key systems, here a single key or a password known only to sender and receiver. Encryption and decryption is possible only if the key is known to both of them. The encrypted message is of the binary image (r x c) size and key is choosen to be a gray scale image size is equal to the binary image (r x c).

S.Maksuanpan and W. San Um [2] published in 2013 5th International Conference on Knowledge and Smart Technology (KST) "A New Simple Digital Image Cryptography Technique Based on Multi Scroll Chaotic Delay Differential Equation". This paper they introduced a new simple digital image cryptography technique based on multi scroll chaotic Delay Differential Equation (DDE) and the proposed technique works only as a simple XOR operation between separated planes of binary gray scale image and a shuffled multiscroll DDE chaotic attractor image. The security keys are parameters in Multi Scroll Chaotic Delay Differential equation and it also include the initial conditions, time constants, and simulation time that sets final states of an attractor. The experiment results are performed in MATLAB using a gray scale image with 512x512 pixels value.

M. Y. R. Gadelha, c. F. F. Costa Filho, M. G. F. Costa [3] published in The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012) "Proposal of a Cryptography Method Using Gray Scale Digital Images". In this paper, a new encryption technique is proposed that uses an image as a key and the main idea behind this technique is use random spatial distribution of pixel gray levels of an image to encrypt text message. The proposed technique is a kind of symmetric key cryptography and the same image is used for both message encryption and decryption.

Smita Pandey [4] published "A novel approach for Digital Image Watermarking Using 5-DWT-SVD and Stream Cipher Encryption with Different Attacks". This paper proposed a novel approach for DIW using five level discrete wavelet transform (5DWT) , singular value decomposition (SVD) and stream cipher (SP) encryption with different attacks..To evaluate the efficiency of the algorithm and the extracted watermark image quality, they use image quality function measurements, signal-to-noise ratio (SNR) and root mean square error (RMSE).

Abhishek Basu, Subhrajit Sinha Roy, Avik Chattopadhyay [5] published in 2016 second International Conference on research in computational intelligence and communication networks (ICRCICN) "Implementation of a Spatial Domain Salient Region Based Digital Image Watermarking Scheme". In this paper, a spatial domain image watermarking scheme is developed through a pixel based saliency map, where the inadequate nature of human visual system is utilized. It encloses a fully spatial domain based algorithm and offering an improved imperceptibility with congruous data capacity and robustness.

Anshul Kanchan Khanna, Nihar Ranjan Roy, Dr. Bhupendra Verma [6] published in International Conference on Computing, Communication and Automation (ICCCA2016) Digital image Watermarking and its optimization using Genetic Algorithm". This paper is an attempt to create an optimal image watermarking scheme for copyright protection that can also resist the common attacks on watermarked image. The watermark is embedded and extracted by 2-level DWT and Genetic algorithm has been employed in the proposed algorithm to find the embedding strength of watermark.

Awadhesh Kumar Yadav, Ruchira Naskar [7] published in 2015 IEEE Power, Communication and Information Technology Conference (PCITC) "A Tamper Localization Approach for Reversible Watermarking based on Histogram Bin Shifting". In this paper, they proposed a tamper localization approach for histogram bin shifting based on reversible watermarking algorithm, where original image will be obtained from the watermarked image with none distortion and it embedded the hash into smaller component part of the image till embedding is feasible .This can facilitate to search out the tampered region at the receiver finish whereas extracting the hash. The case of hash mismatch in cover image which will lead to selective rejection of the cover image.

M. R. Akbarzadeh, S. Ghofrani [8] published "Image Content Authentication and Tamper Localization Based on Semi Fragile Watermarking by Using the Curvelet Transform". In this paper they proposed a semi-fragile image watermarking theme for image authentication and tamper localization. The watermark bits are embedded into coarse level Curvelet coefficients. The extracted watermark is employed to work out whether or not the watermarked image has been changed or not and additionally has the ability to localize the tampered regions. Curvelet transform can represent edges and singularities along curves much more efficiency rather than the traditional wavelet transform, i.e. Accurate reconstruction is obtained by using fewer coefficients.

Chin-Chen Chang, Ngoc-Tu Huynh, Chia-Chun Lin [9] published in 2012 Seventh Asia Joint Conference on Information Security "Strong Tamper-Localization, Visual Secret Sharing Scheme Based on Exploiting Modification Direction". In this paper, they proposed a new, visual, secret-sharing method with high quality shadows by smartly employing a steganography method, it's called Exploiting Modification Direction (EMD), during share construction. This scheme can detect if any tampering has occurred on the shadow and the experimental results show that the scheme is efficient and secure.

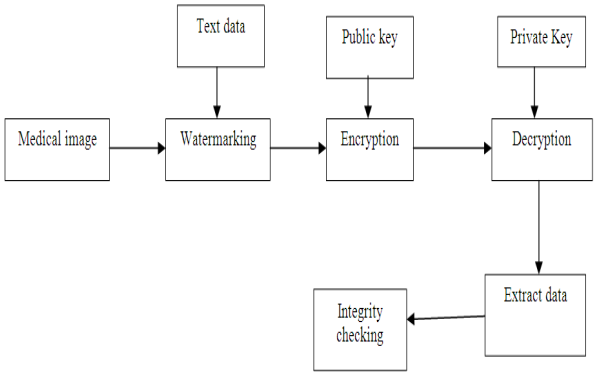
III. PROPOSEDSYSTEM

In this proposed system we combine the watermarking and cryptographic techniques for the medical image secure transmission over the internet. Here we use the combination of DWT and DCT algorithm for watermarking, compare with other techniques this combined version give good PSNR value in the watermarking phase. And the ECDH algorithm is used for the encryption and decryption phase. By using this public key cryptographic technique it provide more security compare with others.

There are mainly three phases in this system:

1. Watermarking phase
2. Cryptographic phase
3. Integrity checking phase

The proposed algorithm is performs as follows: First we select a medical image for transmission over the internet, then perform combined DWT and DCT algorithm for the watermarking purpose. Here we embed the text data such as patients details, hospital name, doctor's id etc. After that we apply the ECDH algorithm for the encryption purpose with public key, then transfer to the receiver. Then the receiver receives the image and decrypt the image using private key and extract the text data from the embedded image. Finally we calculate the integrity of the received image using PSNR calculation.



IV. RESULTS

The following screenshots shows the result of this proposed method. Figure 1 shows the watermarking level 1 and figure 2 shows the watermarking level 2.

Fig. 1. Watermarking level 1

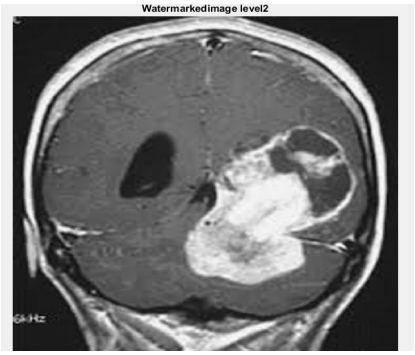


Fig. 2. Watermarking level 2

The figure 3 shows the watermarking final image and figure 4 shows the receiver side process include both decryption and data extraction from the received image.

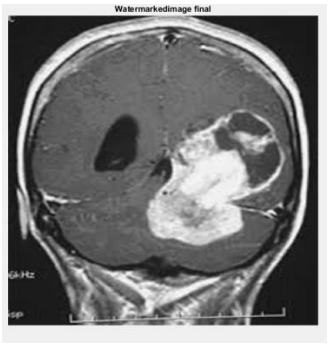


Fig. 3. Watermarked final image

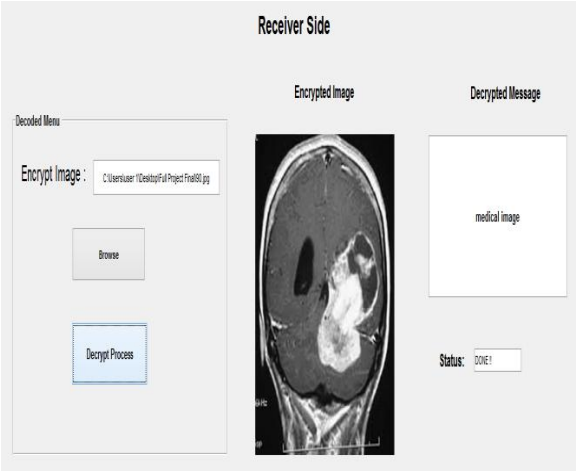


Fig. 4. Receiver side processing

V. CONCLUSION

Nowadays, Telemedicine is used for telecommunication and information technology to provide clinical health care from distance. Information privacy and security issues continue to trouble telemedicine, especially due to the

extensive use of new communication technologies like wireless network in today world. Medical images contain very sensitive information, which should not be made accessible to unauthorized persons in order to protect patient privacy, integrity and confidentiality. In this paper, we propose a combined cryptography and watermarking techniques for secure transmission of medical images. Combined DWT and DCT is used for watermarking and Elliptic curve diffie-helman cryptography is used for encryption purposes. Commonly the DCT and DWT are separately used for watermarking and AES, DES, RSA algorithm are used for cryptographic technique. The proposed system provide good efficiency compared with other techniques because he use of combined DWT and DCT watermarking technique and ECDH algorithm for cryptography.

REFERENCES

[1] Sudip Ghosh, Sayandip De,Santi Prasad Maity, Hafizur Rahaman "A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and cyptography Using Extended Hamming Code", International Conference on Electrical Information and Communication Technology(EICT,2015)

[2] S.Maksuanpan and W. San-Um "A New Simple Digital Image Cryptography Technique Based on Multi-Scroll Chaotic Delay Differential Equation", 2013 5th International Conference on Knowledge and Smart Technology (KST)

[3] M. Y. R. Gadelha, c. F. F. Costa Filho, M. G. F. Costa "Prooposal of a Cryptography Method Using Gray Scale Digital Images ", 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

[4] Smita Pandey, Smita Pandey "A novel approach for Digital Image Watermarking Using 5-DWT-SVD and Stream Cipher Encryption with Different Attacks "

[5] Abhishek Basu, Subhrajit Sinha Roy, Avik Chattopadhyay "Implementation of a Spatial Domain Salient Region Based Digital Image Watermarking Scheme ", 2016 second International Conference on research in computational intellengence and communication networks(ICRCICN)

[6] Anshul Kanchan Khanna, Nihar Ranjan Roy, Dr. Bhupendra Verma "Digital Image Watermarking and its optimization using Genetic Algorithm ", International Conference on Computing, Communication and Automation (ICCCA2016)

[7] Awadhesh Kumar Yadav, Ruchira Naskar "A Tamper Localization Approach for Reversible Watermarking based on Histogram Bin Shifting", 2015 IEEE Power, Communication and Information Technology Conference (PCITC)

[8] M. R. Akbarzadeh, S. Ghofrani "Image Content Authentication and Tamper Localization Based on Semi Fragile Watermarking by Using the Curvelet Transform "

[9] Chin-Chen Chang, Ngoc-Tu Huynh, Chia-Chun Lin "Strong Tamper-Localization,Visual Secret Sharing Scheme Based on Exploiting Modification Direction ", 2012 Seventh Asia Joint Conference on Information Security