VOL. 14, NO. 1, JANUARY 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PROVIDING CONFIDENTIALITY, DATA INTEGRITY AND AUTHENTICATION OF TRANSMITTED INFORMATION

Saleh Suleman Saraireh
Al - Hussien Bin Talal University, Maan, Jordan
E-Mail: saleh_53@yahoo.com

ABSTRACT

Transmission of secret information through non - secure communication channels is subjected to many security threats and attacks. The secret information could be government documents, exam questions, patient information, hospital information and laboratory medical reports. Therefore it is essential to use a strong and robust security technique to ensure the security of such information. This requires the implementation of strong technique to satisfy different security services. In this paper different security algorithms are combined together to ensure confidentiality, authentication and data integrity. The proposed approach involves the combination between symmetric key encryption algorithm, hashing algorithm and watermarking. So, before the transmission of secret information it should be encrypted using the advanced encryption standard (AES), hashed using secure hash algorithm 3 (SHA3) and then embedded over an image using discrete wavelet transform (DWT), discrete cosine transforms (DCT) and singular value decompositions (SVD) watermarking technique. The security performance of the proposed approach is examined through different security metrics, namely, peak signal - to - noise ratio (PSNR) and normalized correlation coefficient (NC); the obtained results reflect the robustness and the resistance of the proposed approach to different attacks.

Keywords: cryptography, watermarking, hashing, authentication, confidentiality.

1. INTRODUCTION

Nowadays the amount of exchanged data has been rapidly increased over wired and wireless communication networks. The transmission of text, audio, image and video is a daily routine over the Internet. It is very popular for users to share huge amount of data through non secure channels. This information is accessible from a third party. Therefore, users need to protect their sensitive data from a third party by using an effective secure system that can satisfy various security services, such as confidentiality, data integrity and authentication. To ensure the security of transmitted information, many techniques can be employed, such as cryptography, hashing and watermarking. Also different techniques can be combined together to obtain a robust and strong secure system.

Cryptography, hashing and watermarking are considered as a popular security algorithms. These algorithms can be applied to provide information security. There are many differences between these algorithms. Cryptography is applied to ensure confidentiality. It converts a readable secret message into a non readable one using advanced mathematical formula for encryption and decryption with a particular key. According to the key, cryptographic algorithms are classified as symmetric key algorithm and public key algorithm [1 and 2]. To ensure data integrity service, hashing algorithm is used, which is a one - way mathematical function that maps a variable length of data into fixed length hash value.

Watermarking is an important and major image processing application. It is considered as a promising solution to protect the copyright of data. It is usually used to satisfy authentication service by embedding information (watermark) over a digital data such as video, audio or an image. The embedded information authenticates the source of the transmitted data. According to the watermarking algorithm, the embedded information can be visible or invisible. Watermarking embedding process can be achieved either in spatial domain or transform domain. The embedded information should not corrupt the quality of the original image. So the watermarked image should be very similar to the original image.

In this paper a hybrid approach is proposed to provide various security services and at the same time to establish a solid ground to implement a secure communication system. The proposed method combines cryptography together with hashing and watermarking. The paper has the following structure: literature review and previous works are introduced in section II. The detail of the proposed algorithm is presented in section III. The results are presented and discussed in section IV and section V mentions the conclusions.

2. LITERATURE REVIEW

To protect the sensitive information and to obtain a high level of security many techniques were proposed. In [2], filter bank based symmetric encryption algorithm was combined with discrete wavelet transform (DWT) based steganography to produce a secure system; the proposed system satisfied only the confidentiality security service. Also in [3], symmetric key algorithm and steganography were merged together to improve the confidentiality.

Integration between MD5 hashing algorithm and DWT based steganography with symmetric cryptographic technique was proposed in [4], the integration was used to satisfy two security services, namely, confidentiality and data integrity. The algorithm proposed in [5] addressed the security of data that involves the transmission of secret image and secret text. So the secret text with its hash value is firstly embedded over the secret image using steganographic algorithm, then the generated stego image is encrypted using symmetric key algorithm.

A combination between encryption algorithm and watermarking techniques was proposed in [6], this combination was proposed to enhance the security of the secret image and at the same time to make copyright protection. Aggregation between discrete cosine transform (DCT) based watermarking and advanced encryption standard was introduced in [7] to satisfy confidentiality and copyright protection. In order to provide authenticity and confidentiality of medical images, Elliptical Curve Diffie Helman (ECDH) public key algorithm was combined with DWT and DCT based watermarking [8].

A hybrid secure system was proposed in [9], the proposed system is used to secure digital images, and it combined cryptography and watermarking, where cryptography was used for pixel displacement and encryption and watermarking for authentication of image. RSA algorithm was employed in [10] to encrypt and sign the secret information, and then the encrypted and signed information were embedded into an image to generate the watermarked image.

In [11], watermarking and cryptography were used together to enhance the security of Digital Imaging and Communication in Medicine (DICOM). This algorithm can be applied in Hospital Data Management Systems (HDMSs) to ensure patient authentication and confidentiality. RSA public key algorithm and DCT based watermarking were used in [12] to secure biomedical images, patient's information, doctor's information and the region of interest (ROI). To improve the security of medical images two level of securities were proposed in [13], these levels include the usage of watermarking and encryption. The watermarking technique based on non tensor wavelet filter banks, it can disclose the singularity in many directions, and the secret information is embedded in LH sub band of the image. A crypto - watermarking algorithm was proposed in [14], the proposed algorithm hided the watermark into region of non - interest using transform domain.

Two dimensional nonlinear chaotic map encryption algorithm was combined with watermarking algorithm to implement a secure image system [15], the implemented approach satisfied the confidentiality and authentication security services. The implemented approach embedded the logo into a host image and then the watermarked image was encrypted using chaotic map algorithm. A hybrid system was proposed based on a combination between a wavelet based watermarking and chaotic map based cryptography [16], so before embedding the watermark in the detail coefficients of the wavelet of the original image, it should be chaotically encrypted. For VoIP system [17], two layers of security were applied; these layers included watermarking and data encryption standard protocol (DES).

Most of the previous works considered only one or two security services. This paper comes to address three security services, namely, confidentiality, data integrity and authentication. This is achieved by combining cryptography, hashing and watermarking.

3. PROPOSED APPROACH AND METHODOLOGY

This section describes the approach in use. It involves the combination of three security techniques, which are hashing, watermarking and cryptographic algorithms as shown in Figure -1. Before the transmission of the secret data, it should be encrypted, hashed and then embedded over an image to generate the watermarked image as explained in Figure-1. The purpose of this combination is to increase the security of the system by satisfying various security services including confidentiality, data integrity and authentication. Confidentiality is achieved by using a particular encryption algorithm, while data integrity is obtained by using hashing algorithm and watermarking technique is applied to satisfy authentication.

Figure-2 shows the sender side. The main operations on the sender side include the following operational steps:

a) Using the AES block cipher with a particular key to encrypt the secret data, as a result the encrypted data is generated. AES is carried out through four steps which are: byte substitution, shift rows, mix columns and add round key. AES can be implemented in hardware or software; also it uses high and scalable key size.

b) Employing the secure hash algorithm 3 (SHA3) to hash the secret data and to generate a 256 bits hash value for a variable input.

c) The hash value and the encrypted secret data are encapsulated together to obtain the concatenated data.

d) The concatenated data is embedded over an image to generate a watermarked image. The embedding process is achieved by employing discrete wavelet transform (DWT), discrete cosine transforms (DCT) and singular value decompositions (SVD) [18].

e) Sending of the watermarked image to the receiver side through a non secure communication channel.

Figure-3 shows the receiver side. At the receiver side the following operational steps are applied:

a) Extraction of the concatenated data from the watermarked image.

b) Obtaining the hash value and the encrypted data by splitting the concatenated data.

c) Decryption of the encrypted data using the same key that used in the encryption process to obtain the corresponding secret data.

d) Computing the hash value of the secret data.

e) Comparing the computed hash value with the received hash value to ensure data integrity. If the hash values are the same, then the data integrity security service is satisfied, otherwise, the data integrity is not satisfied.

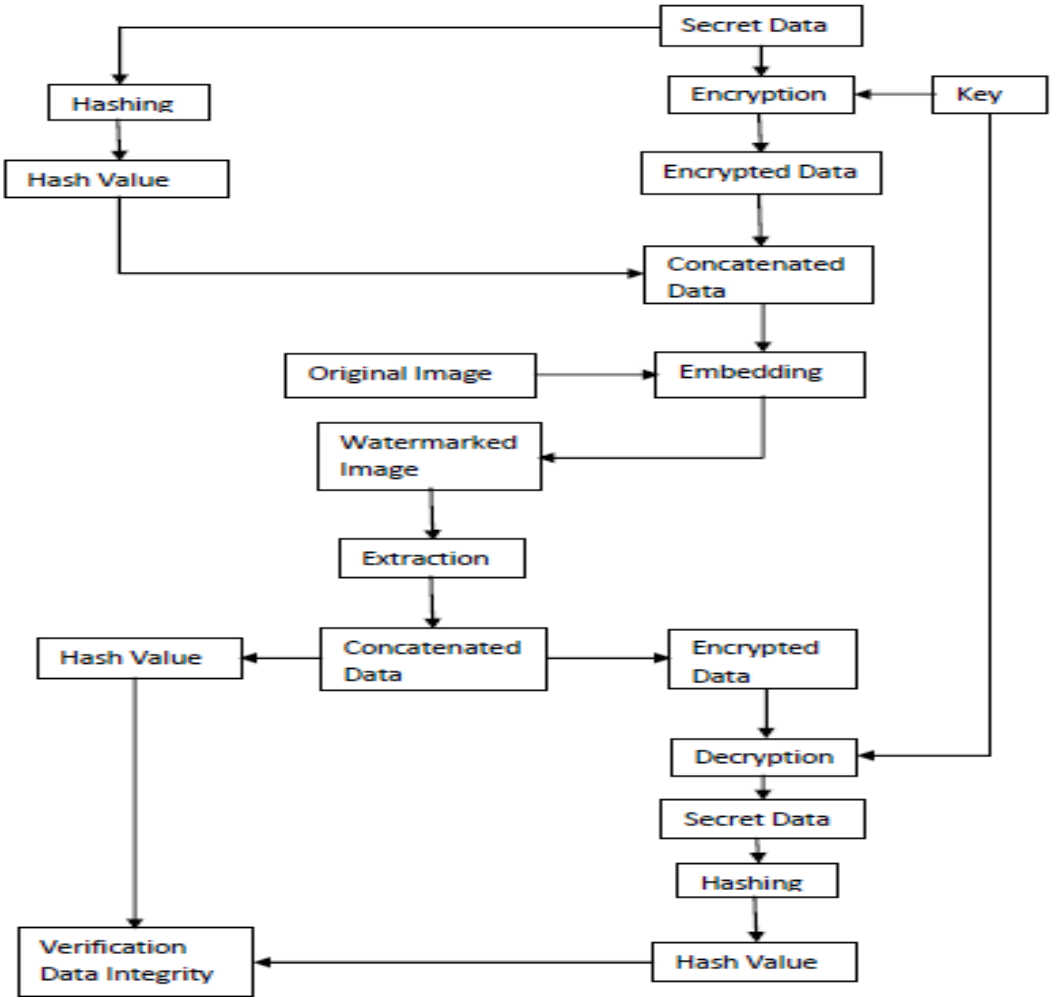


Figure-1. The overall block diagram of the proposed approach.

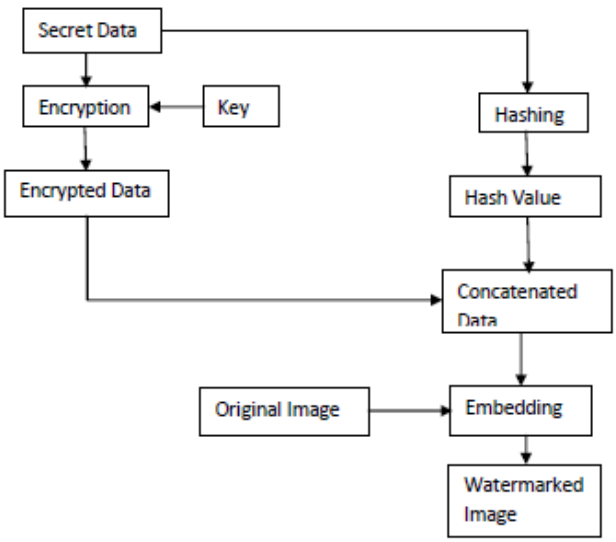


Figure-2. Sender side block diagram.

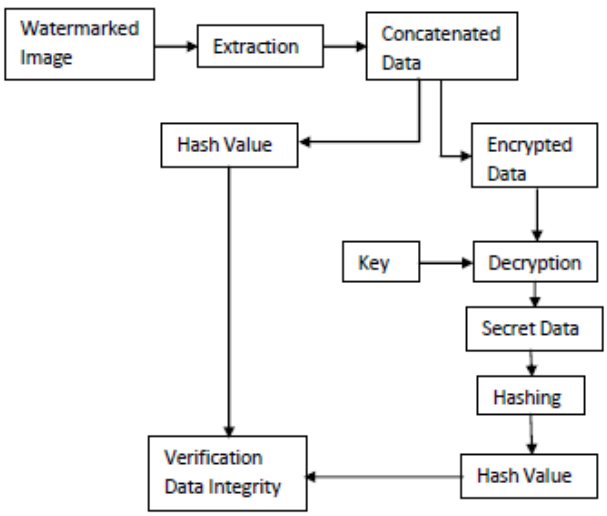


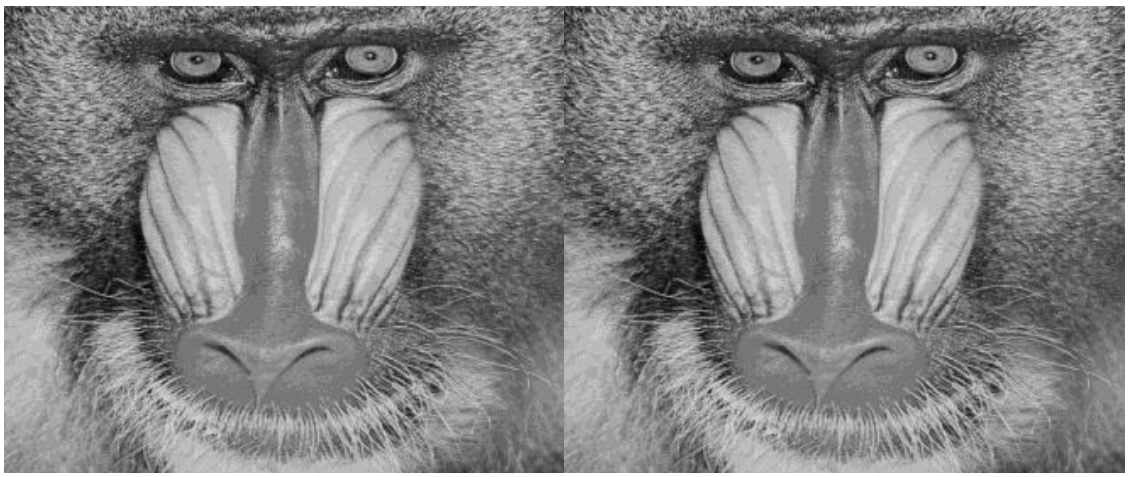
Figure-3. Receiver side block diagram.

4. SIMULATION RESULTS AND DISCUSSION

In order to demonstrate the efficiency and robustness of the proposed approach, different substantial tests are applied using various gray scale images as original or host images. To examine the visual similarity and perceptual quality between the original images and the watermarked images shown in Figure-4 and Figure-5, peak signal - to noise ratio (PSNR) metric is calculated, high PSNR reflects high imperceptibility of the proposed approach. Table-1 indicates that the calculated PSNR values are higher than the recommended 40 dB [19]. This demonstrates the imperceptibility of the proposed approach.

(a) (b)

Figure-4. (a) Lena as an original image. (b) Watermarked image.



(a) (b)

Figure-5. (a) Baboon as an original image. (b) Watermarked image.

Table-1. The calculated PSNR.

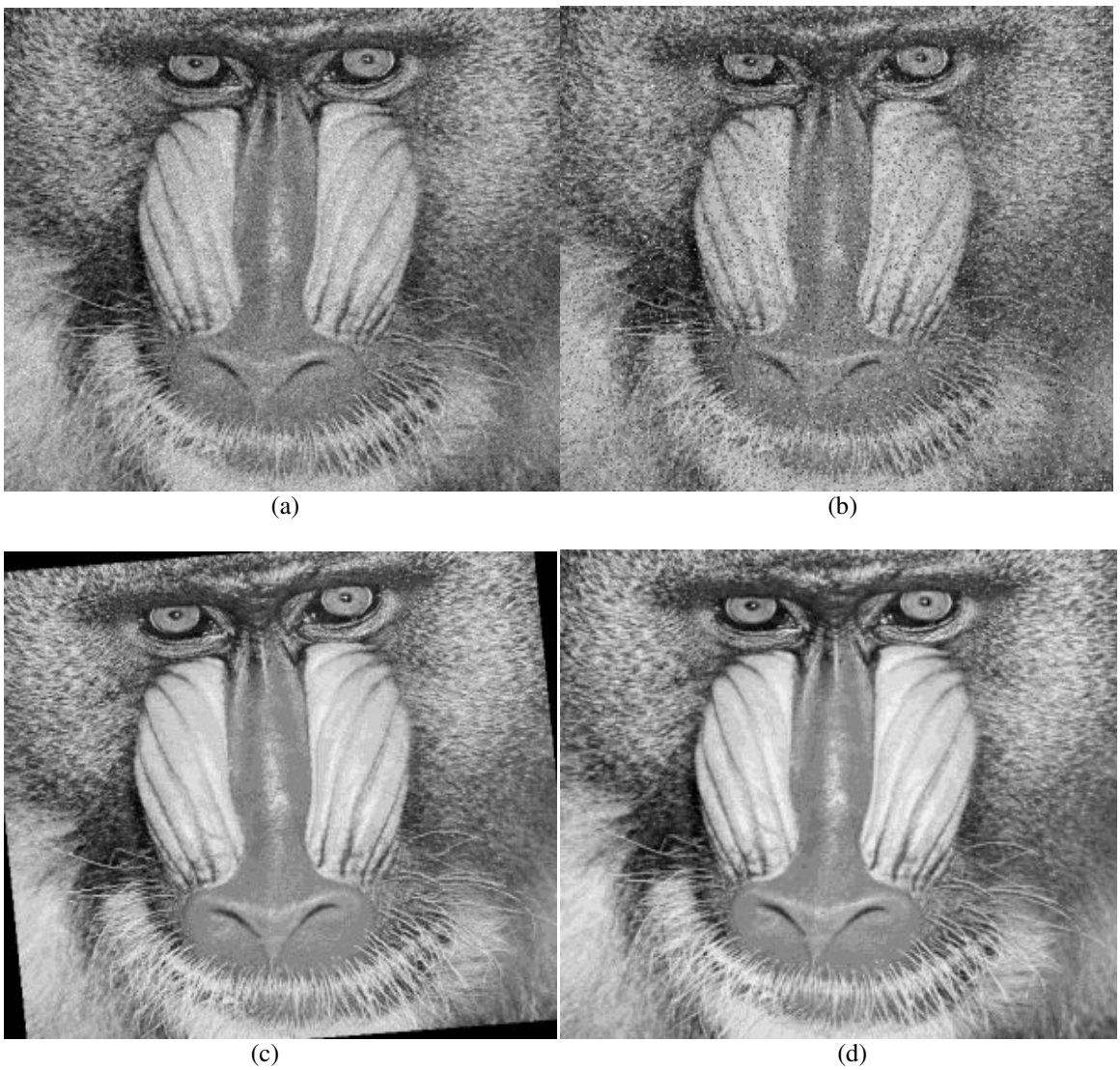
Original image	PSNR dB
Lena	52,32
Baboon	52.45

The transmitted images may be affected by some types modifications, these modifications could corrupt the quality of the watermark that embedded through the original image, so to measure the robustness of the proposed approach, the watermarked images are attacked by Gaussian noise attack, salt and pepper attack, rotation attack and filtering attack as shown in Figure-6 and Figure-7, and the normalized correlation coefficient (NC) is computed. NC is applied to measure the correctness of the extracted watermark and the similarity with the original watermark. The calculated NC values are summarized in Table-2. The calculated NC values are greater than 0.97 which means that the proposed approach withstands against different types of attacks

(a) (b)

(c) (d)

Figure-6. (a) Gaussian noise attack, (b) salt and pepper attack, (c) rotation attack and (d) filtering attack.



(a) (b)

(c) (d)

Figure-7. (a) Gaussian noise attack, (b) salt and pepper attack, (c) rotation attack and (d) filtering attack

Table-2. The calculated values of NC.

Type of the attack	Watermarked image	NC
Gaussian Noise	Lena	0.982
Salt and Pepper		0.972
Rotation		0.997
Filtering		0.993
Gaussian Noise	Baboon	0.973
Salt and Pepper		0.971
Rotation		0.997
Filtering		0.992

To check the validity of the proposed approach, it is compared with other approaches. The proposed approach provides three security services which are confidentiality, authentication and data integrity; on the other hand, the other approaches provide only one or two security services as indicated in Table-3.

Table-3. Comparing the proposed approach with others approaches.

Algorithm	Confidentiality	Authentication	Data integrity
Proposed Approach	Yes	Yes	Yes
[2]	Yes	No	No
[3]	Yes	No	No
[4]	Yes	No	Yes
[5]	Yes	No	Yes
[8]	Yes	Yes	No
[16]	Yes	Yes	No

5. CONCLUSIONS

The proposed approach merges cryptography, hashing and watermarking algorithms to implement a strong and secure technique. It provides three security services, namely, confidentiality, authentication and data integrity. AES cryptographic algorithm is used to provide confidentiality, while SHA3 is employed to provide data integrity and DWT, DCT, and SVD based watermarking is used to provide authentication. The efficiency of the proposed approach is examined and evaluated using PSNR and NC; the calculated values of PSNR are much greater than the recommended standard value (40 dB) which indicates that the proposed approach provides high imperceptibility. Also the calculated values of NC indicate that the proposed approach is secure against Gaussian noise attack, salt and pepper attack, rotation attack and filtering attack.

REFERENCES

[1] Saleh Saraireh, Yazeed Al-sbou, Ja'afer Al-Saraireh and Othman Alsmadi. 2014. Image Encryption Scheme Based on Filter Bank and Lifting. International Journal of Communications, Network and System Sciences (IJCNS,). 7(1).

[2] Saleh Saraireh. 2013. A Secure Data Communication System Using Crptography and Steganography. International Journal of Computer Networks & Communications (IJCNC). 5(3).

[3] Saleh Saraireh and Mohammad Saraireh. 2017. Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange. International Journal on Communications Antenna and Propagation (IRECAP). 7(1): 1-7.

[4] Saleh Saraireh, Jaafer Al-Saraireh, Mohammad Saraireh. 2018. Integration of Hash -Crypto-Steganography for Efficient Security Technique. International Journal of Circuits, Systems and Signal Processing. (12): 274-278.

[5] Saleh Saraireh, J AL-Saraireh, Y Al-Sbou, M Saraireh. 2018. A Hybrid Text - Image Security Technique. Journal of Theoretical and Applied Information Technology. 96(9): 2414-2422.

[6] Sudhanshu Suhas Gonge and Ashok A. Ghatol. 2014. Combination of Encryption and Digital Watermarking Techniques used for Security and Copyright Protection of Still Image, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, 9-11 May.

[7] Sudhanshu Suhas Gonge, Ashok Ghatol. 2016. Aggregation of Discrete Cosine Transform Digital Image Watermarking with Advanced Encryption Standard Technique. Procedia Computer Science. 89: 732.

[8] M. Pooja Prakash, R. Sreeraj, Fepslin Athishmon and Suthendran Kannan. 2018. Combined cryptography and digital watermarking for secure transmission of medical images in EHR systems. International Journal of Pure and Applied Mathematics. 118(8): 265-268.

[9] Kester Q., Nana L., Pascu A. C., Gire S., Eghan J. M., and Quaynor N. N. 2014. A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images based on a Generated Symmetric Key. Int. J. Comput. Appl. 94(19).

[10] Shivi Garg and Manoj Kumar. 2016. Secure Message Transmission Ensuring Authentication Using Digital Signature and Watermarking. International Journal of Computer Science and Information Technologies. 7(1): 413-416.

[11] M. M. Abd-Eldayem. 2013. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. Egyptian Informatics Journal. 14(1): 1-13.

[12] Koushik Pal, Subhajit Koley, Goutam Ghosh and Mahua Bhattacharya. 2013. A New Combined Crypto-Watermarking Technique using RSA Algorithm and Discrete Cosine Transform to Retrieve Embedded EPR from Noisy Bio-Medical Images. K. Pal, *et al*., In: IEEE 1st International Conference on Condition Assessment Techniques in Electrical Systems, IEEE CATCON 2013, Kolkata, December 06 - 08.

[13] A. Kannammal, S. Subha Rani. 2014. Two level security for medical images using watermarking/ encryption algorithms. International Journal of Imaging Systems and Technology. 24(1): 111-120.

[14] Ali Al-Haj, Ahmad Mohammad and Alaa Amer. 2016. Crypto-Watermarking of Transmitted Medical Images. Journal of digital imaging. 30(1): 26-38.

[15] Manaf Mohammed Ali. 2016. Authentication and Secure Image System Based on Combining Image Cryptography and Digital Watermarking. Journal of Kerbala University. 14(1).

[16] Majdi Al-Qdah. 2015. Hybrid Security System based on Wavelet Domain Watermarking and Chaotic Map Cryptography. International Journal of Computer Applications. 110(13).

[17] J Singh, P Garg and A Nath De. 2009. A combined watermarking and encryption algorithm for secure VoIP. Information Security Journal: A Global Perspective. 18(2): 99-105.

[18] Saeid Fazli and Masoumeh Moeini. 2016. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik - International Journal for Light and Electron Optics. 127(2): 964-972.

[19] Ali Al-Haj. 2015. Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. Journal of digital imaging. 28(2): 179-187.