Review of Cryptography Applications in eHealth Security Systems

Rasha Thabit
Universiti Sains Malaysia

International Journal of
Science and Engineering Investigations vol. 8, issue 89, June 2019
Received on June 12, 2019 ISSN: 2251-8843

Review of Cryptography Applications in eHealth Security Systems

Rasha Thabit
Computer Techniques Engineering Department, Al-Rasheed University College, Hay Al-Hussain, Baghdad, Iraq
(rashathabit@yahoo.com)

Abstract- The continuous advance in information technology and digital communication facilitates the process of exchanging the medical information significantly. Nowadays, the eHealth systems are widely used and many prestigious medical centers depend on them in transmitting and receiving the medical information through internet and local networks. Over the years, several security systems have been presented to protect the privacy of the patients and to ensure the safety of the exchanged medical data. Cryptography is one of the techniques that have been used to provide security in eHealth systems. This article presents a review for the recent trends of the cryptography-based security techniques in eHealth systems. The basic concepts and requirements of cryptography in eHealth systems is presented followed by a review of some cryptography-based medical information security techniques which are presented in the last decade. Then, the parameters and metrics that are used to evaluate the implemented cryptography techniques have been reviewed. Thereafter, a summary of the limitations and the recent trends of cryptography applications in eHealth systems is presented. Finally, the conclusions of this review article with some suggestions for future researches in this field are offered.

Keywords- *Cryptography, Medical Data Protection, eHealth Security*

I. Introduction

The advance in information technology and the facilities that can be offered by this technology increased its applications in different important sectors such as the healthcare sector [1]. The eHealth systems store and share different types of health care records such as medical images, electronic patient record (EPR), and other important information which are related to the hospital or the patient. The health care records are shared across the world for different purposes including (but not limited to) the following:

- Telemedicine [2] which refers to the health care service (i.e., diagnosis and treatment) provided for the patients in order to overcome different obstacles such as (distance, cost, time, and efforts).

- Teleradiology [3] which refers to the exchange of radiological patient’s images between radiologists and physicians.

- Telediagnosis [4] which refers to the process of monitoring a distant patient by accessing his/her medical records and diagnosing the disease through distance medical facilities.

- Teleconsultation [5] which refers to the deliberation between doctors or physicians about a specific medical record or case using telecommunication.

Storing and sharing the medical information in their digital form through networks and internet have many advantages as mentioned above therefore the digital medical information became a good alternative to the hardcopies [6]. This medical data is very important and sensitive information and sharing this data through unsecured channel make them vulnerable to different attacks which are not stop at stealing the medical information but also changing this information and sending it back to the receiver. Any change in this information will affect the diagnosis process and consequently the treatment of the patient. Therefore, there is a persistent need to provide security while sharing and exchanging this information in eHealth systems. One of the widely used techniques for ensuring the security and privacy of medical information is cryptography [7] which is a science and art that can change the data from their clear and understandable form to an ambiguous form.

Over the years, different cryptography techniques have been applied to serve the security purposes in eHealth systems. There is always a need for an updated review article to highlight and summarize the recent trends of technology in a specific field, therefore, this article presents a review of the recent trends of cryptography in eHealth systems. The reviewing process mainly focuses on the cryptography applications that have been presented in the last decade for two major types of medical information that are the medical images and electronic patients health records.

The coming sections of the paper are organized as follows: section II presents the basic concepts and requirements of cryptography in eHealth systems, section III presents a review of some cryptography-based medical information security techniques which are presented in the last decade, section IV illustrates the parameters and metrics that are used to evaluate the implemented cryptography techniques, section V contains a summary of the limitations and the recent trends of cryptography applications in eHealth systems, and section VI presents the conclusions of this review paper with some suggestions for future researches in this field.

II. BASIC CONCEPTS AND REQUIREMENTS OF CRYPTOGRAPHY IN EHEALTH SYSTEMS

The corner stone of cryptography techniques is the encryption algorithm that is used to transform the data from its original form to a meaningless form. The original data can be recovered at the receiver side by applying the decryption process using a secret key which is available for only authorized recipient. In order not to compromise the security of the cryptography technique, it is recommended not to save the encryption key on the same server that uses the encryption and decryption algorithms [8]. The encryption process can be classified into two categories that are symmetric and asymmetric according to the key [9, 10]. In symmetric encryption, one key is used which is shared with the receiver in a private and secret way [9]; the larger the size of the key the higher the security of the encryption technique. In asymmetric encryption, two keys are used that are a private key and a public key. Different symmetric and asymmetric encryption algorithms are available to provide security in many digital information applications.

Regarding the digital medical information, there are some basic security requirement that must be accomplished in eHealth security systems which can be epitomized into three main aspects as follows [6, 11, 12]:

- *Confidentiality*: which means the security systems has the ability to restrict the access of medical information to only authorized people.
- *Reliability* (*integrity* and *authentication*): which means the security system can guarantee that the received information has been generated from a trusted source and it has not undergone any modifications.
- *Availability*: which means there should be a scheduled access to the information.

Cryptography is an efficient tool which has been used for saving and transmitting data in a secure manner, however, it cannot meet all abovementioned requirements. Most cryptography techniques in medical information security systems have been presented to fulfill the confidentiality requirements such as the techniques in [9, 13-21]. Some other cryptography techniques have been presented to ensure the integrity and authentication of the medical information [22-24]. To improve the performance of the security system, the cryptography has been combined with data hiding techniques [25-28] and thus the security system can fulfill the requirements that cannot be achieved by the application of the cryptography alone.

The cryptography has been applied to provide security for medical images and patients information. In some cases, the cryptography technique is applied for medical images only [13-21, 24, 27, 28] or for patient’s information only [25]. In other cases, the cryptography is applied for securing both the medical images and patient's information [26]. Sharing the encrypted medical images and patient’s information through telecommunication channels will make them suspicious and they will be vulnerable to the modification attacks. To tackle this situation, some techniques hide the encrypted data in a cover media before sharing it. Fig. 1 presents a general block diagram to summarize the abovementioned medical information security systems that are based on cryptography.

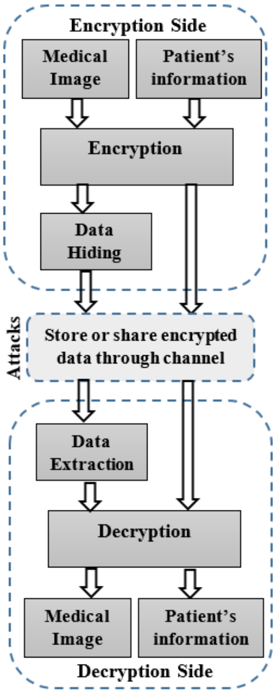

Figure 1. Cryptography-based medical information security system

III. CRYPTOGRAPHY-BASED MEDICAL INFORMATION SECURITY TECHNIQUES

Several cryptography-based techniques have been presented in the last decade to provide security and privacy while exchanging the medical information in eHealth systems. Table I presents the definitions of the acronyms that have been used in the cryptography-based medical information security techniques to facilitate the reviewing process of these techniques.

TABLE I. SUMMARY OF ACRONYMS AND THEIR DEFINITIONS

No.	Acronym	Definition
1	EPR	Electronic Patient’s Record
2	EHR	Electronic Health Record
3	DICOM	Digital Imaging and Communication in Medicine
4	ROI	Region of Interest
5	RONI	Region of non-interest
6	LSB	Least Significant Bit
7	AES	Advanced Encryption Standard
8	GCM	Galois Counter Mode
9	DES	Data Encryption Standard
10	GUI	Graphical User Interface
11	RSA	Ron Rivest, Adi Shamir, and Leonard Adleman
12	CRT	Chinese remainder theorem

Medical images constitute a major part of the medical information which have attracted a lot of interest because of their importance for the monitoring and diagnosis processes. Some cryptography-based techniques have been presented for color medical images. In [9], a color medical image encryption algorithm has been presented which is started by calculating a key for the medical image that depends on its mean and entropy values. The extracted key is used to apply pixel-shuffling process to obtain the encrypted image. This algorithm changed the locations of the pixels without changing their values, therefore, there is no need for the expansion of the image size and the pixel value and this feature can be considered as an advantage of this algorithm. In [13], a lossless color medical image encryption technique has been presented which is based on applying two processes that are the scrambling and confusion. For scrambling the locations of the pixels, the 2D lower triangular map has been used. For confusion process, the paper proposed an algorithm called propeller. In [22], the encryption algorithm from [9] has been combined with watermarking technique in spatial domain for authentication purpose. The encryption process has no effect on the pixel values but the watermark embedding process causes changes in the pixel values of the medical image which is a weakness in this technique. In [15], a medical image security system has been presented in which a random secret key generation process has been applied to obtain the key for the encryption process. The Quantum cryptography, Shor's algorithm and DES, have been used to encrypt and secure the image. The article presented a GUI which shows the original and the encrypted medical images.

Some other cryptography-based techniques have been presented to provide security for DICOM images. In [23], a DICOM image security system has been presented which consists of two stages that are the encryption and signature generation stage and the decryption and signature verification stage. In this technique, the DICOM image is first divided into two regions (i.e., ROI and RONI) and the hash value for ROI is calculated and embedded in the RONI using LSB embedding method. The header of the DICOM image has been encrypted using AES-GCM. At the receiver side, the decryption process is applied then the embedded hash value is extracted from RONI. The new hash value is calculated for the ROI and compared with the extracted one to verify its safety. When the two hash values are different the DICOM image is considered unauthentic. In [14], the homomorphic encryption technique has been applied to provide security for the health care DICOM images that are stored using cloud computing. The image is converted to a matrix and a key is generated to perform the encryption process then the encrypted matrix is converted to an image to be stored in the cloud. In [20], a medical encryption algorithm has been presented that is based on modifying the standard AES algorithm by adding the Arnold's chaotic map as a preliminary step before performing the encryption process. The algorithm has been applied to DICOM images of depth 16 bits. In [24], a feature based encryption scheme has been presented to protect the medical images in cloud computing. The scheme allows multiple users to access the stored DICOM images in cloud using decryption process that is based on verification and authentication procedure.

Some other security techniques are based on chaotic map. In [16], the paper presented a modified chaos-based cryptography algorithm in which 1D standard logistic map has been used to generate a key to encrypt the image. The results of evaluating this method proved that the histograms of the original and the ciphered images are completely different and the histogram of the ciphered image is almost uniform which makes the method robust against statistical attacks and entropy. The disadvantage of this method is the distortions that are presented in the recovered image after the decryption process. In [18], a medical image security system depends on a secret key and chaotic mapping has been presented. The medical image is divided into blocks of size (16×16 pixels) and mixing process has been applied to shuffle the blocks in horizontal and vertical directions.

In [17], an encryption algorithm based on using sub-keys from a secret key for randomly changing the locations of the pixels and their values has been presented. Two rounds of encryption process have been applied to increase the security. The scheme has robustness against different attacks and it can be applied for different image modalities. This technique has robustness to define noise and data loss. In [19], a dual encryption method is applied to encrypt the medical images where the Blowfish Encryption is first applied followed by signcryption algorithm. Then, private and public keys are upgraded using the Opposition based Flower Pollination (OFP). In [21], a security technique has been presented for medical images transmission and storage in cloud computing. This technique based on compressing the medical image using Huffman coding and encrypting the image using Blowfish encryption method.

Some other techniques combine cryptography with data hiding techniques (i.e., steganography and watermarking) to obtain better security performance. In [25], the patient's information has been encrypted using RSA algorithm and three different embedding methods have been applied to hide the encrypted sequence in the medical image. The first method depends on applying visible watermarking process which embeds the sequence in a corner of the medical image. The second and third methods depends on using LSB and discrete cosine transform (DCT) based embedding processes. In [26], a medical image security scheme based on watermarking and cryptography has been presented. First, a secret message is encrypted using Caesar shift ciphering method and embedded in the edges of the medical image in order not to affect the ROI. The resultant watermarked image has been encrypted using Chinese remainder theorem (CRT). In [27], the medical image is converted to binary sequence and the secret data is embedded in the LSBs of the image's binary sequence. The resultant sequence is then encrypted using Blowfish encryption. At the receiver side the Blowfish decryption is first applied followed by the extraction process of the secret data. In [28], different combinations of cryptography and watermarking techniques have been studied to achieve the combination that can give the best results. The medical image has been encrypted using RSA and AES algorithms. Then, the encrypted image has been embedded in a cover image using Lifted wavelet transform (LWT) and singular value decomposition (SVD).

Table II presents a summary of the cryptography-based medical information security techniques that have been reviewed in this section in terms of the type of the protected medical information, the cryptography technique, and the data hiding technique in case if it is utilized.

TABLE II. SUMMARY OF THE REVIEWED TECHNIQUES IN THIS SECTION

Technique	Protected information	Cryptography technique	Data Hiding technique
Q. Kester, 2013 [9]	Color medical image	Pixel-shuffling	×
N. O. Abokhdair, et. al., 2010 [13]	Color medical image	Scrambling and confusion	×
A.M. Vengadapurvaja, et. al., 2017 [14]	DICOM image	Homomorphic encryption	×
O. D Alowolodu, et. al., 2018 [15]	Medical image	Quantum cryptography	×
M. T. Gatta, & S. T. Abd Al-latief, 2018[16]	Medical image	Chaotic-based encryption	×
H. Zhongyun, et. al., 2018 [17]	Medical image	Sub-keys and pixel shuffling	×
R. Gupta, et. al., 2018 [18]	Medical image	Chaotic-based and block of pixels shuffling	×
T. Avudaiappan, et. al., 2018 [19]	Medical image	Blowfish and signcryption	×
R. S. Bhogal, et. al., 2018 [20]	DICOM image	Modified AES	×
M. L. Singh & T. Senthilnathan, 2018 [21]	Medical image	Blowfish	×
Q. Kester, et. al., 2015 [22]	Color medical image	Pixel-shuffling	Watermarking in spatial domain
K. S. Aparna, 2016 [23]	DICOM image	AES-GCM	LSB embedding
A. M. Badr, et. al., 2019 [24]	DICOM image	Feature based encryption	×
M. YANG, et. al., 2010 [25]	Patient’s information	RSA	Visible watermarking, LSB, and DCT
A. Mahmood, et. al., 2013 [26]	Medical image & Secret data	CRT	Image partitioning and invisible watermarking
C. D. Naidu, et. al., 2014 [27]	Medical image	Blowfish	LSB embedding
CH. V. Reddy & P. Siddaiah, 2015 [28]	Medical image	RSA and AES	LWT and SVD

IV. THE PARAMETERS AND METRICS FOR PERFORMANCE EVALUATION

The application of cryptography techniques to medical information in eHealth systems must pass some benchmarking limits. This section illustrates the parameters and metrics that can be used to evaluate the performance of the cryptography techniques in eHealth systems. Then a summary of the parameters and metrics that have been used in the articles [9, 13-28] is presented in Table III.

A. *The encrypted image (EI)*

After applying the encryption algorithm to the medical image, the encrypted image is displayed to illustrate the visual difference between the original medical image and its encrypted version. The more different the images, the better the performance of the encryption algorithm.

B. *The watermarked image (WI)*

After embedding data in the cover image using watermarking technique, the resultant watermarked image is displayed to illustrate the visual difference between the original image and its watermarked version. The less different the images, the better the performance of the watermarking technique.

C. *Histogram and RGB graphs analysis*

The histogram analysis process is a way to illustrate the distribution of the pixels in an image. The encrypted image must have a uniformly distributed histogram. The more uniform the histogram, the better the performance of the encryption technique because it will be difficult to extract the pixel’s statistical nature of the original medical image [14]. For the color medical images, the RGB graphs are shown which represent the histograms of the three channels of the color image (i.e., Red, Green, and Blue) [9, 22].

D. *Key space analysis*

The secret key of the encryption algorithm of length L-bits has a key space of length 2^L. The larger the key space, the more secure the encryption technique but it is at the cost of increasing the volume of the hardware and reducing the speed of the system.

E. *Lossless analysis*

The application of cryptography and data hiding techniques on medical images can present distortions in the image. These techniques are called lossless when the distortions can be removed and the original image can be recovered at the receiver side. For lossless analysis, the pixels of original medical image and the recovered image after decryption or data extraction are compared to illustrate if there is any difference between them.

F. *Entropy analysis*

The entropy is a measure of randomness and unpredictability [16] which can be calculated using (1):

$$H(m) = -\sum_{I=0}^{2^N-1} P(m_i) log_2 P(m_i) \quad (1)$$

Where m_i is the pixel value in the image m, P is the probability of existence of the gray level value of the pixel m_i.

In case of grayscale images, the ideal entropy value for secure cryptography system should be 8. The encryption technique that can obtain entropy value near 8 has more resistance against entropy attacks [16, 29].

G. MSE and PSNR

The mean square error (MSE) and the peak-signal-to-noise ratio between two images I_1 and I_2 of size $M \times N$ can be calculated using (2) and (3), respectively.

$$MSE = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I_1(i,j) - I_{2(i,j)})^2 \tag{2}$$

$$PSNR(I_1, I_2) = 10 \times log_{10} \frac{MAX_I^2}{MSE} \tag{3}$$

Where MAX_I is the maximum possible pixel value of the image I .

These metrics are used to evaluate the performance in different cases as follows:

- To compare the original medical image and the encrypted image. In this case, the lower the $PSNR$ value, the better the performance. The lower $PSNR$ value means more difference between the original image and encrypted image.
- To compare the original medical image and the recovered image after the decryption process. In this case, the higher the $PSNR$ value, the better the performance. The higher $PSNR$ value means more similarity between the original image and recovered image.
- To compare the original medical image and the watermarked image. In this case, the higher the $PSNR$ value, the better the performance. The higher $PSNR$ value means more similarity between the original image and watermarked image.

H. Correlation coefficient analysis

The correlation coefficient is a statistical metric used to measure the relationship between two variables and how much they altered with each other. The correlation coefficient (CC) range is between (+1 and -1). When the calculated CC value is near (+1), the pixels of the two images are positively correlated and both of them simultaneously increase or decrease. When the calculated CC value is near (-1), the pixels of the two images are negatively correlated and they are inversely related [14, 18]. The correlation coefficient (CC) can be calculated using the following equation:

$$CC = \frac{N \sum_{j=1}^{N} (x_j * y_j) - \sum_{j=1}^{N} x_j * \sum_{j=1}^{N} y_j}{\sqrt{(N \sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2) * (N \sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \tag{4}$$

Where x and y are the two neighboring pixels and N is the number of pixels in the image.

To evaluate the performance of the encryption technique, the CC values for neighboring pixels in the encrypted images are calculated in three directions that are the vertical, horizontal, and diagonal directions. The performance of the encryption technique is better when the obtained CC values near zero.

I. Time analysis

Time analysis is an important evaluation metric which refers to the time required for the encryption and decryption processes to be executed. The time is increased with the increment of the system complexity [16]. The less the execution time, the better the performance of the cryptography technique.

J. Number of pixel change rate (NPCR)

The number of pixel change rate (NPCR) is a metric used to measure the ability of an encryption algorithm to resist differential attacks. Suppose C$_1$ and C$_2$ are two cipher-images encrypted from two plain-images with only one-bit difference, NPCR is defined as [17]:

$$NPCR(C_1, C_2) = \sum_{i,j} \frac{A(i,j)}{G} \times 100\% \tag{5}$$

Where G is the total number of pixels in each cipher-image, and A represents the difference between C_1 and C_2 which can be calculated as follows:

$$A(i,j) = \begin{cases} 0, \ if \ C_1(i,j) = C_2(i,j), \\ 1, \ if \ C_1(i,j) \neq C_2(i,j). \end{cases} \tag{6}$$

TABLE III. SUMMARY OF THE PARAMETERS AND METRICS THAT HAVE BEEN USED IN THE ARTICLES [9, 13-28]

Technique	The parameters and metrics
Q. Kester, 2013 [9]	EI, and RGB graphs
N. O. Abokhdair, et. al., 2010 [13]	Key space and lossless analysis
A.M. Vengadapurvaja, et. al., 2017 [14]	EI, key space, Histogram, MSE, PSNR, and Correlation analysis
O. D Alowolodu, et. al., 2018 [15]	No evaluation metrics
M. T. Gatta, & S. T. Abd Al-latief, 2018 [16]	EI, histogram, entropy, and time analysis
H. Zhongyun, et. al., 2018 [17]	EI, key analysis, and NPCR
R. Gupta, et. al., 2018 [18]	EI, correlation, NPCR, MSE, and PSNR analysis
T. Avudaiappan, et. al., 2018 [19]	Entropy, Correlation, MSE, and PSNR
R. S. Bhogal, et. al., 2018 [20]	EI, histogram, time, and Correlation.
M. L. Singh & T. Senthilnathan, 2018 [21]	PSNR
Q. Kester, et. al., 2015 [22]	EI, RGB graphs, entropy and mean values
K. S. Aparna, 2016 [23]	EI, and WI
A. M. Badr, et. al., 2019 [24]	EI, Time, MSE and PSNR
M. YANG, et. al., 2010 [25]	No evaluation metrics
A. Mahmood, et. al., 2013 [26]	EI, WI, histogram, entropy, and PSNR
C. D. Naidu, et. al., 2014 [27]	Time, MSE and PSNR
CH. V. Reddy & P. Siddaiah, 2015 [28]	WI, correlation, MSE, and PSNR

V. SUMMARY OF THE LIMITATIONS AND THE RECENT TRENDS

There are several security risks that can face the sensitive data while they are transmitted from their source to destination via internet such as rootkits, SQL injection, session hijacking, session prediction and others which increased the need for cybersecurity [30]. Cryptography is one of the techniques that have been used in cybersecurity systems, however, it suffers from some limitations. Saving and exchanging data in their encrypted form can attract the attention and increase the suspicion about the importance of this data and thus it will be more vulnerable to different attacks. To avoid this limitation, the recent trends of cryptography techniques are towards hiding the encrypted data in a cover media. On the other hand, the data embedding techniques are useful in hiding the existence of the secret data but they are at the cost of increasing the complexity of the system and the processing time. Another trend of cryptography techniques is their application to ensure security in cloud computing [8]. In addition, the cryptography techniques for color medical images have also gained a growing interest because of their spreading in comparison with traditional grayscale medical images.

VI. Conclusions

This review article has been presented to provide an insight for the recent trends of cryptography-based security techniques in eHealth systems. The cryptography techniques have been successfully applied to provide security in eHealth systems, however, they have some limitations which can be avoided by combining them with other security techniques such as data hiding techniques. On the other hand, the combination of cryptography and data hiding is at the cost of increasing the complexity and the processing time, therefore, there should be a compromise according to the requirements and the priorities of the security system.

There are different metrics and parameters that can be used to evaluate the performance of the cryptography techniques for medical data. The researcher how is interest in presenting a new cryptography technique for medical data should consider these metrics when evaluating the implemented technique to prove its efficiency. The recent trends of security systems in eHealth are the security of medical information in cloud computing and the security of color medical images, therefore, the researchers how are interested in the topic of this review article may directed their efforts towards these topics.

References

[1] Gutierrez, M. A., Moreno, R. A., Rebelo, M. S. (2017). Chapter 3 - Information and Communication Technologies and Global Health Challenges. Global Health Informatics, Academic Press, 50-93.
https://doi.org/10.1016/B978-0-12-804591-6.00004-5

[2] Whitten, P. et al. (2010). Telemedicine: What have we learned?. Applied clinical informatics. 1(2). 132-41.
http://dx.doi.org/10.4338/ACI-2009-12-R-0020

[3] Krupinski, E. A. (2014). Teleradiology: current perspectives. Reports in medical imaging. 7. 5-14.
https://doi.org/10.2147/RMI.S48140

[4] Aupet, J. B., Garcia, E., Guyennet, H., Lapayre, J. C., Martins, D. (2010). Security in Medical Telediagnosis. In: Tsihrintzis G.A., Jain L.C. (eds) Multimedia Services in Intelligent Environments. Smart Innovation, Systems and Technologies. 3. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/978-3-642-13396-1_9

[5] Deldar, K., Bahaadinbeigy, K., Seyed, M. T. (2016). Teleconsultation and Clinical Decision Making: a Systematic Review. ACTA INFORM MED. 24(4): 286-292.
https://doi: 10.5455/aim.2016.24.286-292

[6] Nyeem, H., Boles, W., Boyd, C. (2013). A Review of Medical Image Watermarking Requirements for Teleradiology. J Digit Imaging. 26.326–343.
https://doi.org/10.1007/s10278-012-9527-x

[7] Stallings, W. (2013). Cryptography and network security principles and practice. 6th edition, Pearson Education, Inc., Prentice Hall, 752 pages.
https://www.amazon.com/Cryptography-Network-Security-Principles-Practice/dp/0133354695

[8] Vululleh, P. (2019). Applying Cryptography to Ensure Cloud Computing Security. International Journal of Science and Engineering Investigations (IJSEI), 8(85), 74-76.
http://www.ijsei.com/papers/ijsei-88519-12.pdf

[9] Kester, Q. MIEEE. (2013). A visual cryptographic encryption technique for securing medical images. International Journal of Emerging Technology and Advanced Engineering, 3(6).
https://arxiv.org/ftp/arxiv/papers/1307/1307.7791.pdf

[10] Costa, D. G., F. Solenir, G. Oliveira. (2017). Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions. Cryptography, 1(4).
doi:10.3390/cryptography1010004.

[11] Winkler, T., Rinner, B. (2014). Security and Privacy Protection in Visual Sensor Networks: A Survey. ACM Comput. Surv. 47. 97–116.

[12] S. C., Liew, J. M., Zain. (2009). A Review of Medical Image Watermarking Schemes. Proceedings of ICSECS09, International Conference on Software Engineering and Computer Systems, Pahang, Malaysia.
https://www.researchgate.net/publication/282610498_A_Review_of_Medical_Image_Watermarking_Schemes

[13] N. O., Abokhdair, A., Abdul Manaf, M., Zamani. (2010). Integration of chaotic map and confusion technique for color medical image encryption. 6th International Conference on Digital Content, Multimedia Technology and its Applications, Seoul. 20-23.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5568578&isnumber=5568515

[14] A. M. Vengadapurvaja, G. Nisha, R. Aarthy, N. Sasikaladevi. (2017). An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security", Procedia Computer Science. 115. 643-650.
https://doi.org/10.1016/j.procs.2017.09.150.

[15] O. D., Alowolodu, G. K., B. K., Adelaja, Alese, O. C., Olayemi, (2018). Medical image security using quantum cryptography. Issues in Informing Science and Information Technology, 15, 57-67.
https://doi.org/10.28945/4008

[16] M. T., Gatta and S. T., Abd Al-latief. (2018). Medical image security using modified chaos-based cryptography approach. IOP Conf. Series: Journal of Physics: Conf. Series 1003. 012036.
doi :10.1088/1742-6596/1003/1/012036

[17] Z., Hua, S., Yi, Y., Zhou. (2018). Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing. 144. 134-144, ISSN 0165-1684.
https://doi.org/10.1016/j.sigpro.2017.10.004

[18] R., Gupta, R., Pachauri, A. K. Singh. (2018). An Effective Approach of Secured Medical Image Transmission Using Encryption Method. MCB Molecular and Cellular Biomechanics 15(2). 63-83.
DOI: 10.3970/mcb.2018.00114

[19] T., Avudaiappan, R., Balasubramanian, S.S., Pandiyan, et al. (2018). Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm. J Med Syst. 42(208). https://doi.org/10.1007/s10916-018-1053-z

[20] R. S., Bhogal, B., Li, A., Gale, Y. Chen. (2018). Medical Image Encryption using Chaotic Map Improved Advanced Encryption Standard. I. J. Information Technology and Computer Science, 8, 1-10,

DOI: 10.5815/ijitcs.2018.08.01

[21] M. L., Singh, T., Senthilnathan. (2018). ANALYSIS OF SECURE CLOUD STORAGE PROVISIONING FOR MEDICAL IMAGE MANAGEMENT SYSTEM. International Journal of Mechanical Engineering and Technology (IJMET). 9(3), 162–173.

[22] Q., Kester, L. Nana, A. Christine Pascu, Sophie Gire, Jojo M. Eghan, Nii Narku Quaynor, A Cryptographic Technique for Security of Medical Images in Health Information Systems, Procedia Computer Science, Volume 58, 2015, Pages 538-543, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.08.070

[23] K. S., Aparna, R., Sreejith, A. T., Ambikadevi. (2016). An Advanced Crypto Based Security System for Medical Image/Data Transfer. 5(6).

[24] A. M., Badr, Y., Zhang, H., Umar. (2019). Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloud Computing. Electronics, 8 (171).

doi:10.3390/electronics8020171

[25] M., YANG, et. al. (2010). Secure Patient Information and Privacy in Medical Imaging. SYSTEMICS, CYBERNETICS AND INFORMATICS. 8(3).

[26] A., Mahmood, C., Obimbo, T., Hamed, R., Dony. (2013). Improving the Security of the Medical Images. (IJACSA) International Journal of Advanced Computer Science and Applications. 4(9).

[27] C. D., Naidu, S., Koppu, V. M., Viswanatham, S. L., Aarthy. (2014). Cryptography based medical image security with LSB Blowfish algorithms. ARPN Journal of Engineering and Applied Sciences. 9(8).

[28] V., Reddy, P., Siddaiah. (2015). Hybrid LWT-SVD watermarking optimized using metaheuristic algorithms along with encryption for medical image security. Signal & Image Processing: An International Journal (SIPIJ). 6(1).

[29] J. ,Ahmad, A., Fawad. (2012). Efficiency analysis and security evaluation of image encryption schemes Inter. Journal of Video and Image Processing N.W. Sec. 12(25).

[30] Vululleh, P. (2019) Cybersecurity Issues in Online Learning. International Journal of Science and Engineering Investigations (IJSEI), 8 (87), 96-100.

http://www.ijsei.com/papers/ijsei-88719-14.pdf

Dr. Rasha Thabit received her B.Sc. degree in Electronics and Communications Engineering from University of Baghdad, Iraq, in 2006, and M.Sc. degree in Electrical Engineering from University of Baghdad, Iraq, in 2008. She received her Ph.D. degree in Software Engineering from the School of Electrical & Electronic Engineering at Universiti Sains Malaysia (University of Science, Malaysia), in 2015. Her research interest is in the area of data hiding, digital information security, digital image watermarking, and digital signal processing.

How to Cite this Article:

Thabit, R. (2019) Review of Cryptography Applications in eHealth Security Systems. International Journal of Science and Engineering Investigations (IJSEI), 8(89), 110-116. http://www.ijsei.com/papers/ijsei-88919-16.pdf