International Journal of
Science and Engineering Investigations vol. 9, issue 103, August 2020
Received on August 21, 2020 ISSN: 2251-8843

Review of Medical Images Security Approaches

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

Abstract- The rapid spread of technology and the benefits that can be obtained from utilizing it caused a radical change in the modern health care systems. The easiness of creating, storing, and sharing digital medical images makes them a good alternative to the hardcopies. Storing and exchanging digital medical images save time, cost, and efforts, however, they are under the threat of reaching to unauthorized person who may modify them. Malicious attacks and modifications on medical images before reaching their destination will affect the final diagnosis and decision results, therefore, there is a persistent need to protect digital medical images while exchanging them through unsecure channel. Over the years, different approaches have been applied to provide security while exchanging digital medical images. This paper presents a review of different medical images security techniques and their trends in the last decade. The paper compares between the objectives, properties, and requirements of the reviewed techniques in order to provide an overview for the students, readers, and researchers to understand which approach is more suitable for their applications which are related to medical images security purposes.

Keywords- *Medical Images Security, Cryptography, Data Encryption*

I. INTRODUCTION

The eHealth services are increasing and spreading day after another because of their advantages for the physicians and patients such as saving time, reducing cost and efforts, and obtaining the opinions from experts who may live in a place far away from the hospital or the patient. These services provide the chance for the users to easily remote access the medical images for the diagnosis purposes. The benefits of using these services may be vanished if the medical images accessed by unauthorized people, therefore, several security issues are raised in this field [1-4]. The security requirements can be summarized as follows:

- The sender and receiver of the medical images should have the same level and criterion for security and privacy management.
- The access and storage of the medical information, the process of sharing them, and all the directive rules should be controlled by a suitable authorization process.
- There are five main security requirements as shown in Figure 1 which are required in the security systems that are used for storing or sharing the medical images.

Figure 1. Medical images security requirements

The confidentiality characteristic refers to the ability of the system to provide access to the data by only specific users while the availability means there should be a scheduled access to the information which must be followed by the users to get that information. The integrity of the medical images refers to the ability of the system to ensure the safety of these images from unauthorized modifications [1-3]. The authenticity is the ability of the system to confirm that the medical images have been generated from a trusted source and are received from the right patient while the non-repudiation refers to the protection against disavowal by the people who share the medical information through the system [4].

Several medical imaging security approaches and techniques have been presented to achieve the previously mentioned requirements. The cryptography and data hiding techniques are examples of the widely used approaches for security purposes in medical imaging systems. The cryptography is a science and art of encoding the secret information in order to change the original information from their obvious form to an ambiguous form [5]. Data hiding techniques are classified as steganography and watermarking according to the relationship between the cover image and the secret data that are embedded in the image [6]. The data hiding technique called steganography when the secret data is the part that needs protection. In this case, the secret data is embedded in a cover image which is usually not related to the data and it is only used as a means to carry the secret data in a secure manner. The data hiding technique called watermarking when the cover image is the part that needs protection and in this case the secret data is always related to the cover image [7]. Figure 2 illustrates the difference between steganography and watermarking based medical imaging security approaches.

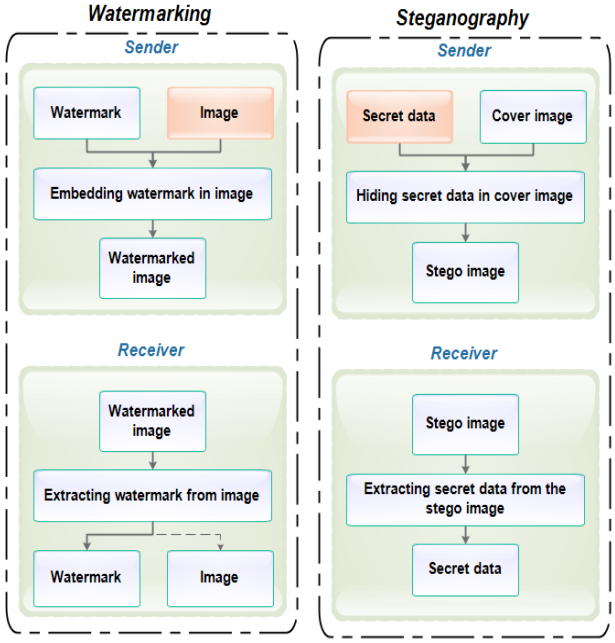

Figure 2. The difference between steganography and watermarking based security approaches

Most of medical imaging security systems rely on the watermarking based approaches because the medical images are the type of data that needs to be protected. As shown in Figure 2, in watermarking based approach, the medical image can be recovered at the receiver side and in this case the watermarking technique is called reversible (i.e., lossless or revertible). The rest of the paper is organized as follows: the next section contains an over view for the review articles that are related to medical imaging security approaches and techniques; section III focuses on the security of medical images based on cryptography; section IV presents the conclusions of this paper.

II. Review Articles for Medical Imaging Security Approaches and Techniques

Over the years, several review articles have been presented to highlight the security issues and review different techniques that can be applied for medical images security purposes. Some review articles that are presented in the last decade can be found in [4], [8]-[18]. In 2009, the review article in [8] highlighted the security requirements, the medical images quality, and reviewed a few number of medical image watermarking techniques. In 2010, a brief review article concentrated on the necessity of using lossless techniques to provide security in medical images [4]. The lossless process means the modifications that are applied on the image should be completely reversible and the original medical image can be recovered correctly. In 2013, a brief review of medical images steganography techniques has been presented in [9]. The review focused on the effect of steganography methods on the visual quality of the medical images. The article concluded that the steganography process give rise to perceptual changes in the medical images. At the same year, another review article has been presented in [10] which contains a review of teleradiology security requirements. The article reviewed different watermarking techniques in teleradiology and highlighted their requirements, pros, and cons.

In 2014, a valuable review article has been presented in [11] which reviewed different medical image watermarking techniques in spatial domain and transform domain. The article also presented a review of the performance analysis methods and evaluation parameters that can be used to evaluate the implemented watermarking technique. In 2015, a review article has been presented in [12] to illustrate the security requirements while sharing or storing the medical information using mobile computing devices. The article also presents a discussion and comparison for different encryption methods that can be applied to provide security between computer networks. During the same year another article [13] reviewed some watermarking techniques for medical image in addition to the medical images modalities.

In 2016, different encryption algorithms for medical images have been reviewed briefly in [14]. During the same year, two other review articles have been presented to review the medical image watermarking techniques, their requirements, and purposes [15, 16]. In 2017, an article reviewed different watermarking techniques which have been presented to protect the electronic patients record (EBR) [17]. In 2019, an article presented an overview for the attacks and requirements of medical image watermarking techniques, in addition, some watermarking techniques have been reviewed and their importance in health care systems has been highlighted [18]. Table I summarizes the review articles in the last decade which have been mentioned before.

There is always a necessity to supply the research community with updated review articles to provide better insight to the recent trends in a specific research field. As shown in Table 1 most of the review articles in the last decade have focused on data hiding techniques, therefore, there is a need for an updated review article that focused on cryptography techniques for medical images. This article

presents a review of different medical images security systems that have been presented in the last decade which are based on cryptography. The following section contains a review of medical images security techniques based on cryptography, their capabilities, advantages, and limitations. Thereafter, the conclusions and suggestions for future research are elucidated.

TABLE I. A SUMMARY OF THE REVIEW ARTICLES IN [4], [8]-[18]

Review Article	The focus of the review article	Some available information in the article
L. S. Chuin, & J. M. Zain, 2009 [8]	Watermarking	Watermarking requirements, performance measures, and embedding domains
S. Rohini, & V. Bairagi, 2010 [4]	Lossless data hiding	Data hiding requirements
P. Kamal, & G. Jinda, 2013 [9]	Steganography	performance measures, and embedding domains
H. Nyeem et al., 2013 [10]	Watermarking	Security and Privacy Requirements in Teleradiology, limitations of existing security measures/tools, and advantages and disadvantages of watermarking
S. M. Mousavi et al., 2014 [11]	Watermarking	Watermarking applications and requirements, embedding domains, Watermarking Benchmarks and Performance Analysis
A. F. Choudhri et al., 2015 [12]	Steganography	Performance measures, and embedding domains, limitations of some steganography techniques
N. H. Ghazali et al., 2015 [13]	Watermarking	Medical image modalities, watermarking applications, literature review of some authentication techniques and their characteristics
N. Hamidipour & A. Sarmeydani, 2016 [14]	Cryptography	Literature review of some medical image encryption techniques
K. Kaur & E.S. Kaur, 2016 [15]	Watermarking	Literature review of some medical image watermarking schemes that are used for authentication, data hiding, or both
P. Kishore et al. [16]	Watermarking	Types of attacks on security systems, watermarking requirements, literature review of several medical image watermarking techniques
G. Singh, 2017 [17]	Watermarking	Literature review of watermarking techniques for embedding EPR in medical image
A. H. Allaf, & M.A. Kbir, 2018 [18]	Watermarking	Types of attacks on security systems, watermarking requirements

III. SECURITY OF MEDICAL IMAGES BASED ON CRYPTOGRAPHY

Different cryptography techniques have been applied as a means to provide security while exchanging medical images through internet or other unsecured channels. Figure 3 shows a general block diagram for the medical images security systems that are based on cryptography. As shown in Figure 3 the cryptography scheme consists of two stages that are the encryption and decryption processes.

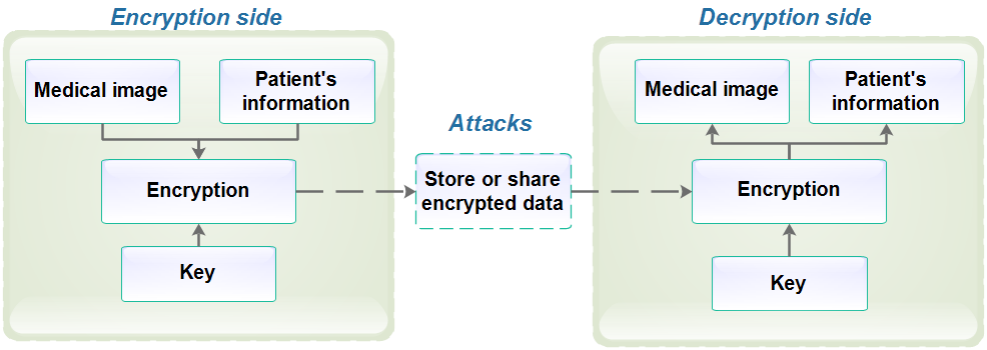

Figure 3. The difference between steganography and watermarking based security approaches

The cryptography scheme can be used for security of medical image or patient's information or both. For instance, in [19], an encryption algorithm has been applied to color medical images. The image's mean and entropy values are calculated to generate a key which is used to apply pixel-shuffling process. This algorithm changed the pixels' locations of the medical image without changing their values. The advantage of this method is that there is no need for the expansion of the image size and the pixel value. In [20], two processes have been applied to obtain the encrypted image which are the scrambling and confusion methods. Two-dimensional lower triangular map method has been used for scrambling the locations of the pixels

and the propeller method has been used for the confusion. In [21], a random secret key has been generated using Quantum cryptography, Shor's algorithm, and Data Encryption Standard (DES). The generated key has been applied to encrypt and secure the medical image and a Graphical User Interface (GUI) has been implemented to show the original and the encrypted medical images. In [22], the homomorphic encryption technique has been applied to provide security for a specific type of images called Digital Imaging and Communication in Medicine (DICOM) images which are stored using cloud computing. The algorithm starts by converting the medical image into a matrix and a key is generated to perform the encryption process. The resultant encrypted matrix is then converted to image to be stored in the cloud. In [23], a DICOM medical image encryption algorithm has been presented that is based on modifying the Advanced Encryption Standard (AES) algorithm by adding the Arnold's chaotic map as a preliminary step before performing the encryption process. 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.

In [25], a cryptography technique based on chaos method has been applied to generate a key for encrypting the medical image. The experimental results of this technique proved that the histograms of the encrypted images are almost uniform and this feature makes the technique more robust against statistical attacks. This method suffers from the problem of the distortions that are generated in the recovered image after applying the decryption process. In [26], a chaotic-based medical image encryption algorithm has been applied which is started by dividing the image into blocks and shuffling the blocks in the horizontal and vertical directions according to a secret key. In [27], a cryptography technique has been presented based on randomly changing the locations of the pixels by using sub-keys that are generated from a secret key. To increase the security of this technique, two rounds of encryption have been applied. The technique can be used to provide security for different image modalities and it has robustness against different attacks. In [28], a cryptography technique based on dual encryption method has been applied to encrypt the medical images. In this technique the Blowfish encryption is applied followed by signcryption algorithm. Thereafter, the private and public keys of the encryption algorithm are upgraded using the Opposition based Flower Pollination (OFP) method. In [29], a security technique has been offered for medical images exchange and storage through cloud computing. In this technique, the medical image is compressed using Huffman coding and encrypted using Blowfish encryption process.

TABLE II. SUMMARY OF THE CRYPTOGRAPHY TECHNIQUES IN [19]-[29]

Reference	Type of medical image	Encryption type	Capability	Advantages	Limitations
[19]	Color image	Pixel-shuffling	Lossless Confidentiality	No need for expansion in image size and pixel value	Non uniform histogram of encrypted image which means less robustness against statistical attacks
[20]	Color image	Scrambling and confusion	Lossless Confidentiality	Robust against brute-force and statistical attacks	High time complexity
[21]	DICOM image	Homomorphic encryption	Confidentiality	Long key which improves the robustness against brute-force	Non uniform histogram of encrypted image which means less robustness against statistical attacks
[22]	Grayscale image	Quantum cryptography	Confidentiality Authenticity	A modified Shor's algorithm and DES improved the security of the technique	High time complexity
[23]	Grayscale image	Chaotic-based encryption	Confidentiality	The use of chaotic maps improved the robustness against attacks	Distortions are generated in the decrypted medical image
[24]	Grayscale image	Sub-keys and pixel-shuffling	Confidentiality	High security, improved speed and robustness	Not mentioned in the article
[25]	Grayscale image	Chaotic-based and block of pixels shuffling	Confidentiality	Almost uniform histogram of the encrypted image which improved the robustness against statistical attacks	Distortions are generated in the decrypted medical image
[26]	Grayscale image	Blowfish	Confidentiality	Almost uniform histogram and the use of different keys improved the security of the technique	Distortions are generated in the decrypted medical image and high time complexity
[27]	DICOM image	Modified AES	Confidentiality	Almost uniform histogram of the encrypted image which improved the robustness against statistical attacks	High time complexity
[28]	Grayscale image	Blowfish	Confidentiality	Less storage space in cloud because of using Huffman coding	High time complexity
[29]	DICOM image	Feature based encryption	Confidentiality Authenticity	verified and authenticated decryption process for the cloud environment	High time complexity

As illustrated in Table II, the cryptography techniques can achieve one or two from the security requirements (i.e., confidentiality and authenticity) that have been shown in Figure 1. To achieve more security requirement, the cryptography techniques alone are not enough and they may be combined with data hiding techniques to obtain better performance.

IV. CONCLUSIONS

This paper starts by briefly presenting the review articles that are related to the topic of medical images security using cryptography and data hiding techniques. Followed by a review of cryptography techniques that have been presented in the last decade to provide security for medical images. The security requirements that can be achieved using cryptography are the confidentiality and authenticity. The advantages and limitations of these techniques have been summarized.

As explained in this review, the recent trends of the medical images security techniques are directed towards color medical images and security of medical images in cloud computing. Therefore, the new cryptography techniques can focus on the requirements of these fields. To provide more security, it is recommended to mix the cryptography technique with the data hiding techniques.

REFERENCES

[1] P. Ruotsalainen "Privacy and security in teleradiology". European Journal of Radiology, vol. 73, pp. 31–35, 2010. https://doi.org/10.1016/j.ejrad.2009.10.018

[2] C. Tan, J. Ng, X. Xu, C. Poh, Y. Guan, and K. Sheah. "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability". Journal of Digital Imaging, vol. 24, pp. 528–540, 2011. https://doi.org/10.1007/s10278-010-9295-4

[3] N.A. Memon, A. Chaudhry, M. Ahmad, and Z.A. Keerio. "Hybrid watermarking of medical images for ROI authentication and recovery". International Journal of Computer Mathematics, vol. 88, pp. 2057–2071, 2011. https://doi.org/10.1080/00207160.2010.543677

[4] S. Rohini, and V. Bairagi, "Lossless Medical Image Security". INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, Vol. 1, No. 3, pp. 536-541, 2010. http://www.ipublishing.co.in/jarvol1no12010/EIJAER2022.pdf

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

[6] F.Y. Shih. "Digital Watermarking and Steganography: Fundamentals and Techniques". Second Edition, CRC Press, 270 Pages, April 26, 2017.https://www.crcpress.com/Digital-Watermarking-and-Steganography-Fundamentals-and-Techniques-Second/Shih/p/book/9781498738767

[7] A.K. Singh, M. Dave, and A. Mohan. "Wavelet Based Image Watermarking: Futuristic Concepts in Information Security". Proc. Natl. Acad. Sci., India, Sect. A Phys. Sci. vol. 84, no. 345, 2014. https://doi.org/10.1007/s40010-014-0140-x

[8] L.S. Chuin, and J.M. Zain. "A Review of Medical Image Watermarking Schemes". Proceedings of ICSECS09, International Conference on Software Engineering and Computer Systems, Oct19-21, 2009, Pahang, Malaysia.https://www.researchgate.net/publication/282610498_A_Review_of_Medical_Image_Watermarking_Schemes

[9] P. Kamal, G. Jindal. "Review of Different Steganographic techniques on Medical images regarding their efficiency". International Journal of Innovations in Engineering and Technology (IJIET), vol. 2, no. 1, 2013. https://pdfs.semanticscholar.org/5edb/a7b901c91696addee439bc2f197b3587b5fa.pdf

[10] H. Nyeem, W. Boles, and C. Boyd. "A Review of Medical Image Watermarking Requirements for Teleradiology". Journal of Digital Imaging, vol. 26, pp. 326–343, 2013. https://doi.org/10.1007/s10278-012-9527-x

[11] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar. "Watermarking Techniques used in Medical Images: a Survey", Journal of Digital Imaging, vol. 27, pp. 714–729, 2014. https://dx.doi.org/10.1007%2Fs10278-014-9700-5

[12] A. F. Choudhri, A. R. Chatterjee, R. Javan, M. G. Radvany, and G. Shih. "Security Issues for Mobile Medical Imaging: A Primer". Radio Graphics, vol. 35, no. 6, pp.1814–1824, 2015. https://doi.org/10.1148/rg.2015140039

[13] N. H. Ghazali, A. A. Manaf, and G. Sulong. "Review of Watermarking Techniques for Medical Images". International Journal of Applied Engineering Research, vol. 10, no. 2, pp. 4991-5003, 2015.https://www.researchgate.net/publication/282187004_Review_of_watermarking_techniques_for_medical_images

[14] N. Hamidipour, and A. S. Sarmeydani. "Advances in Medical Image Encryption". Journal of Electronics and Communication Engineering Research, vol. 1, no. 1, 2016.https://www.researchgate.net/publication/311231309_Advances_in_Medical_Image_Encryption

[15] K. Kaur, and E. S. Kaur. "Review of Image Watermarking Technique for Medical Images", International Journal of Advance research, Ideas and Innovations in Technology, vol. 2, no. 5, 2016.

[16] P. V. V. Kishore et al. "MEDICAL IMAGE WATERMARKING: RUN THROUGH REVIEW", ARPN Journal of Engineering and Applied Sciences, vol. 11, no. 5, 2016. http://www.arpnjournals.org/jeas/research_papers/rp_2016/jeas_0316_3735.pdf

[17] G. Singh. "A review of secure medical image watermarking" 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 3105-3109.https://doi.org/10.1109/ICPCSI.2017.8392297

[18] A.H. Allaf, M.A. Kbir. "A Review of Digital Watermarking Applications for Medical Image Exchange Security". Innovations in Smart Cities Applications Edition 2. SCA 2018. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-11196-0_40

[19] Q. M. Kester. "A visual cryptographic encryption technique for securing medical images". International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 6, 2013. https://arxiv.org/ftp/arxiv/papers/1307/1307.7791.pdf

[20] N. O. Abokhdair, A. Abdul Manaf, and M. Zamani. "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, 2010.http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5568578&isnumber=5568515

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

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

[23] R. S. Bhogal, B. Li, A. Gale, and Y. Chen. Medical Image Encryption using Chaotic Map Improved Advanced Encryption Standard. I. J. Information Technology and Computer Science, 8, 1-10, 2018. DOI: 10.5815/ijitcs.2018.08.01

[24] Z. Hua, S. Yi, and Y. Zhou. "Medical image encryption using high-speed scrambling and pixel adaptive diffusion". Signal Processing, vol. 144, pp. 134-144, 2018. https://doi.org/10.1016/j.sigpro.2017.10.004

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

[26] R. Gupta, R. Pachauri, and A. K. Singh. "An Effective Approach of Secured Medical Image Transmission Using Encryption Method". MCB Molecular and Cellular Biomechanics, vol. 15, no. 2, pp. 63-83, 2018. DOI: 10.3970/mcb.2018.00114

[27] T. Avudaiappan, R. Balasubramanian, S.S. Pandiyan, et al. "Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm". J Med Syst. Vol. 42, no. 208, 2018.https://doi.org/10.1007/s10916-018-1053-z

[28] A. M. Badr, Y. Zhang, H. Umar. "Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloud Computing". Electronics, vol. 8, no. 171, 2019. Doi:10.3390/electronics8020171

[29] M. L. Singh, and T. Senthilnathan. "ANALYSIS OF SECURE CLOUD STORAGE PROVISIONING FOR MEDICAL IMAGE MANAGEMENT SYSTEM". International Journal of Mechanical Engineering and Technology (IJMET), vol. 9, no. 3, pp. 162–173, 2018.

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. Currently she is working as a lecturer in computer techniques engineering department, Al-Rasheed university college, Hay Al-Hussain, in Baghdad, Iraq. 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. (2020). Review of Medical Images Security Approaches. International Journal of Science and Engineering Investigations (IJSEI), 9(103), 45-50. http://www.ijsei.com/papers/ijsei-910320-10.pdf