A Contribution to Enhance the Panoramic Image Security via Cryptography and Shuffled Methods

[1]AAMIR SHAHZAD, [2]SUNGHO KIM, [3]YONGSUNG KIM, [4]MALREY LEE, [5]HYANGRAN LEE
[6]GISUNG JEONG
[1,2,3,4,5] 561-756, Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, Chon Buk, KOREA.
[6] Department of Fire Service Administration, WonKwang University, REPUBLIC OF KOREA

Abstract: - Major changes have been accounted in the field's of information technology(IT), the information that may in the form of audio, video and text, can be transferred anytime, from source to destination or vice versa that may located in anywhere in the World. The evolutions that have been made in the communication sectors, such wire and wireless networks, brought many merits for the end-users prospects, but at the same time, several vulnerabilities and threads have also been linked simultaneously with, and during the information exchanges. To keep the information secure before transmits from the source and receives at the destination, two generic security solutions are proposed which provide a significance security for the information that being travelled in the unsecure networks. First solution uses the cryptography mechanisms while the second solution employs a novel shuffling method, which deployed to enhance the security of information while travelling to the unsecured networks. In this study, the random sized panoramic images are considered as information that required to be secured over internet.

Key-Words: - Security Attack, Panoramic Image Security, Cryptography, Shuffled method.

1 Introduction

Nowadays, the information that may in the forms of audio, video, text and images, can be transferred by the use of communication media, such as wire and wireless, which provide the efficient, and fast delivery; but at the same time, numbers of security threads have also been resided in between the transmission(s) [1—5]. Formal security methods, such as steganography and visual cryptography, are deployed to hide the information of digital images while travelling to the open networks [1, 2]. A study by Jasni Zain et al., the telemedicine system used an

Table. 1 Security Attacks and Vulnerabilities [5]

Attacks	Integrity Attacks, Authentication Attacks, confidentiality Attacks, Non-Repudiation Attacks , Unauthorized Access Control, Bot-network operators, Criminal groups, Phishers, Spammers Spyware/malware, etc.
Vulnerabilities	Inadequate security policy , No formal ICS security Inadequate security architecture, Lack of security administrative, no security audits, Lack of configuration, No proper OS and application security, Lack of adequate password policy Inadequate access controls applied, Inadequate testing of security changes, Insecure remote access on ICS components, Use of insecure industry-wide ICS protocols, Incidents are not detected, Malware protection software not installed, Weak network security architecture, Poorly configured security equipment, Passwords are not encrypted in transit, Inadequate access controls applied, No security perimeter defined, Inadequate firewall and router logs, No security monitoring on the ICS network, Lack of integrity checking for communications, Authentication of users, Inadequate authentication between clients and access points, Inadequate data protection between clients and access points and others.

integrated merits of information technology (IT) and telecommunication, telemedicine information (i.e., patient data) always required a se curity and transmission over internet for the purpose of fast and reliable delivery. Thus, watermarking and steganography techniques are suggested that provided security for medical images [1].
Table 1 shows the number of attacks and common vulnerabilities that mainly resided in the informative networks [6]. Like others', images are also accounted as unsecured form of information and will require a security solution that protect them from the networks adversaries. Chae Hongseok el at., proposed a cryptography based security mechanism that further distributed in main three algorithms, such as AES, RSA and SHA-2, for the information protection [6]. Puech et al., also analyzed the weaker security level of information and then proposed two security dimensions that keep the information of digital images and videos' to be secured. The first dimension focus to keep the information secured against the outside attackers that would become a parts of normal processing, while second dimension classified the main cryptograph algorithms and their use for multimedia contents (protections) [7, 8].

2 Proposed work and Implementation

To keep the information secure that is in the form of images, the potential security mechanisms are proposed that will have significance measurements against network adversaries [9—12]. In first security mechanism, the cryptography algorithms, AES and SHA-512, are employed to secure the images that planned to transmit over the open networks or internet. AES is a symmetric algorithm of cryptography and has same security key that shared between two participated nodes and provides security parameters against the confidentiality and authentication attacks. The AES security key or secret key is first generated and then shared with the target node via secure channel that ensured its uniqueness and security [9]. Therefore, at the both sides a same shared secret key will be employed during encryption and decryption processes. Algorithm 1 shows the panoramic image's deployed security via symmetric AES algorithm

2.1 Algorithm 1: Security Development via Symmetric AES

i. Select the random size panoramic image or images and designated as 'Img'.

ii. Generate a secret key, and shared this key between the participated nodes.

iii. Use step i and deployed the AES algorithm for encryption process at sender (S) side. Then transmits it to the target (T) side.

iv. At target side, use step i and ii for decryption process.

v. Ensure the information, and test the confidentiality and authentication security goals.

vi. End of algorithm.

The SHA-512 algorithm generates a fixed size short code for the desired information (i.e., panoramic images) that is ready to transmit over the internet or networks and is a part of cryptography. This algorithm is deployed to secure the information against integrity based adversaries and has been accounted as a m ost efficient and convenient algorithm due to its merits. Algorithm 2 shows the panoramic image's deployed security via SHA-512 cryptography algorithm.

2.2 Algorithm 2: Security Development via SHA-512 Hashing

i. Select the random size panoramic image or images and designated as 'Img'.

ii. Generate a fixed size hash value (H) or hash digest (H) for selected image (Img), then transmits it to the target (T) side.

iii. At target side, repeat step i and then compares with sender hash digest.

iv. Check and ensure the comparison output, and test the information for integrity security goals.

v. End of algorithm

As the cryptography based mechanisms are considered as costly and complex solutions, but have strong security paradigms against potential networks adversaries. Therefore, a solution is proposed to utilize the best performs of cryptograph, the AES symmetric algorithm and SHA-512 hashing algorithm are deployed together that will measure the more efficient security performances for panoramic images (against adversaries). Moreover, this security solution will also be optimal due to the used of both algorithms (such as AES and SHA-512). Algorithm 3 shows the panoramic image's

deployed security by combined effort of AES and SHA-512 algorithms.

2.3 Algorithm 3: Security Development via Optimal Approach

i. Select the random size panoramic image or images and designated as 'Img'.

ii. Generate a secret key, and shared this key between the participate nodes.

iii. Use step i and deployed the AES algorithm for encryption process at sender (S) side.

iv. Generate a fixed size hash value (H) or hash digest (H) for secret key.

v. Then transmit to the target (T) side.

vi. At target side, repeat step iv,and then compare with sender as: .

vii. If shared secret key match then use this key for decryption process.

viii. Ensure the information, and test the confidentiality, authentication, integrity security goals.

ix. End of algorithm.

A novel security mechanism is proposed that secure the information of panoramic images through the uses of shuffling method. In this method, the random sized panoramic images are selected, and each selected image is converted into the number of small pieces, means that, each image has converted into 'n' number of pieces. These pieces are then further shuffled also in the number of times, the shuffling method (or algorithm) keeps the tracks of that numbers in-which selected image was converted and shuffled. Upon receiving at the target side, the shuffling method is deployed to view the desired information that will be in the form of image(s). This method is most convenient and has required two main steps that provide the security for panoramic images while travelling over the unsecured media. The detail description of shuffling method can also be looked in Algorithm 4.

2.4 Algorithm 4: Security Development via Shuffling Method

i. Select the random size panoramic image or images and designated as 'Img'.

ii. Convert the selected image into the number of 'n' pieces (p), logical distribution as.

iii. Use step ii and shuffle (F) it in 'n' number of times (t), as then transmits it as a payload message.

iv. At target side, use same method to open a sender(S) payload message, after implementing the shuffling and distribution processes.

v. End of algorithm.

3 Results and Discussion

The assurance of information delivery and also keep its contents secure from the networks vulnerabilities and attacks, it is important to have an efficient and reliable security mechanism that will be powerful in-protection of information. The cryptography based mechanisms have been considered as excellent approaches for secure information delivery, therefore, the current work has used the cryptography algorithms and also deployed a novel shuffling method, which provided significant security measurements for the selected panoramic images. Table 2 shows the total approximate sessions that have computed via optimal approach for the random size panoramic images.

Table. 2 Performances

No.	Image Size(bytes)	Optimal Approach: AES and SHA-512	Security Test
1.	9,548	9000 ms	Verified
2.	8,987	8300 ms	Verified
3.	13,220	11500 ms	Verified
4.	13,174	11000 ms	Verified
5.	16,193	13000 ms	Verified
6.	11,757	10000 ms	Verified
7.	10,593	9600 ms	Verified
8.	13,512	11800 ms	Verified
9.	4,815	3000 ms	Verified
10.	7,948	7000 ms	Verified
11.	12,064	10300 ms	Verified
12.	9,689	9100 ms	Verified

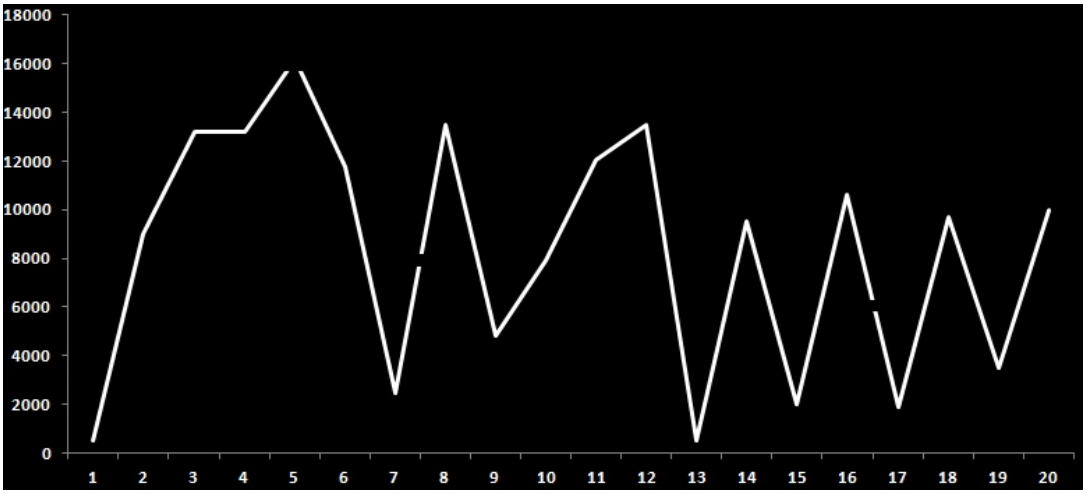

Fig. 1 Transmission Flows via Optimal Method

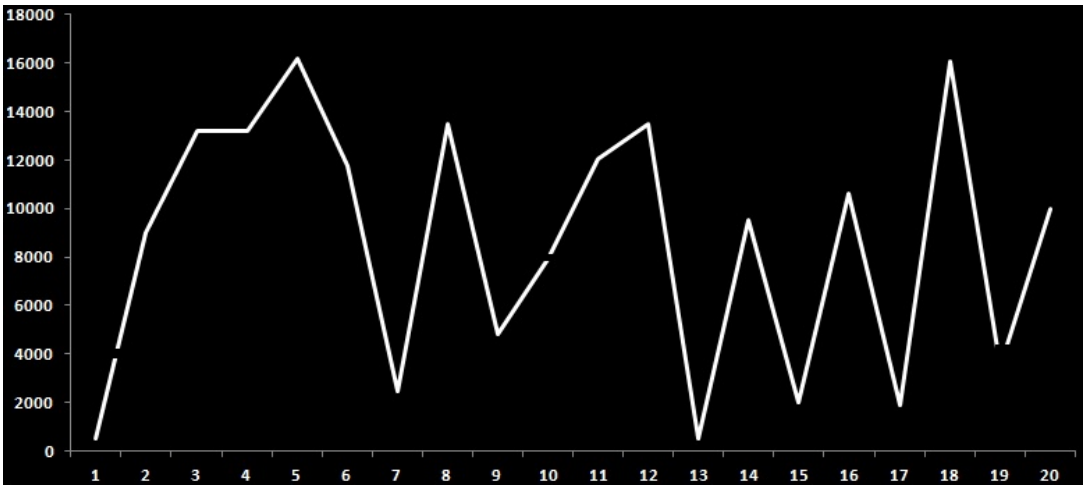

Fig. 2 Transmission Flows via Shuffling Method

In addition to above results, the transmission flows are also monitored to check the communication flows during the random size panoramic images were transmitted. Performance figures 1and 2 show the transmission flow sequences in-case of normal flow that represented by sequential lines and error counted flow that represented by a sm all gap in between the transmission.

4 Conclusion and future work

The modern enhancements such are the part of information technology sectors are useful and bring many advantages of easy, reliable, and efficient access for the human lives, but at the same time, they have several issues in the terms of security that would be interacted with the information that being exchanged by two or multiple networked nodes. The current study uses two security mechanisms, such as cryptography method and shuffling method, that applied and the measured results are efficient and significant in-protection of information against the network or Internet adversaries. In future, the proposed security methods will be employed for industrial images that will also have required security because the almost parts of industrial infrastructures (e.g., oil, gas, power and water plants) and their processing are monitored and controlled over the internet access where the proprietary and the non-proprietary protocols are interconnected and networked.

Acknowledgment

This work (Grants No: 1401001175) was supported by Business for Academic-industrial Cooperative establishments funded Korea Small and Medium Business Administration in 2015.

References:

[1] Khizrai, Mohammad Sajid Qamruddin, and S. T. Bodkhe, "Image Encryption using Different Techniques for High Security Transmission over a Network.", *International Journal of*

Engineering Research and General Science, Vol.2, No.4, 2014, pp. 299-306.

[2] Nivedhitha, R., Dr T. Meyyappan, and M. Phil, "Image Security Using Steganography and Cryptographic Techniques.", *International Journal of Engineering Trends and Technology*, Vol.3, No.4, 2012, pp 366-371.

[3] Zain, Jasni, and Malcolm Clarke, "Security in telemedicine: issues in watermarking medical images.", *The 3rd International Conference: Science of Electronic, Technologies of Information and Telecommunications,* 2005.

[4] Patel, Bhumi, and R. C. Patel, "Overview of watermarking and cryptography to combine both for real time speech communication.", *International Journal of Science, Engineering and Technology Research*, Vol.3, No.2, 2014, pp 279-285.

[5] Shahzad. A, Lee. M, Lee. Y.K, Kim. S, Xiong. N, Choi. J.Y and Cho. Y, "Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information." *Symmetry*, Vol.7, No.3 2015, 1176-1210.

[6] Chae Hongseok, AAmir Shahzad, Muhammad Irfan, HyangRan Lee, and Malrey Lee. "Industrial Control Systems Vulnerabilities and Security Issues and Future Enhancements.", *Advanced Science and Technology Letters*, Vol.95, 2015, pp. 144-148.

[7] Madan Singh, Arvind Kumar and Kehar Singh, "Encryption by using matrix-added, or matrix-multiplied input images placed in the input plane of a double random phase encoding geometry", *Opt Laser Eng*, Vol.47, No.11, 2009, pp. 1293-1300.

[8] El Sawda. R, Al Falou. A, Keryer. G and Assoum. A, "Image Encryption and Decryption by Means of an Optical Phase Mask," *Information and Communication Technologies*, Vol.1, 2006, pp.1474-1477.

[9] Lu Ming-Xin, Lai Xue-Jia, Xiao Guo-Zhen and Qin Lei, "Symmetric Key Cryptosystem with DNA Technology", *Science in China Series F: Information Sciences*, Vol.50, No.3, 2007, pp. 324-333.

[10] Musheer Ahmad and M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping.", *International Journal on Computer Science and Engineering,* Vol.2, No.1, 2009, pp. 46-50.

[11] Aamir Shahzad, Kalum Priyanath Udagepola, Young-keun Lee, Soojin Park and Malrey Lee, "The Sensors Connectivity within SCADA Automation Environment and New Trends for Security Development during Multicasting Routing Transmission.", *International Journal of Distributed Sensor Networks*, Vol.2015, pp. 1-15.

[12] J. Fridrich, "Image Encryption Based on Chaotic Maps", *IEEE International Conference on Systems, Man, and Cybernetics, Computational Cybernetics and Simulations*, Vol.2, 1997, pp.1105 -1110.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0
https://creativecommons.org/licenses/by/4.0/deed.en_US