*International Journal of Advanced Smart Convergence Vol.5 No.1 23-29 (2016)*
*http://dx.doi.org/10.7236/IJASC.2016.5.1.23*

IJASC 16-1-4

# A study of keep the Secret information of Random Sized Images from using Indestructible Security

Seon-mi Woo*, Malrey Lee** and Hyang Ran Lee**,+

**JINI Co., Ltd, B-102, Technobill, 109 banryong-road, Deokjin gu, Jeonju, Chon Buk, Korea*
smwoo@chonbuk.ac.kr
***,+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*
mrlee@chonbuk.ac.kr, orange1469@naver.com

***Abstract***

*The information is to be considered as important part of any network, the communication nodes within network can able to communicate and transmit information by the means of configured LAN/WAN, or/and using internet technology. Thus, vast enhancement has been made in- exchanging of information over transmission media, this should be beneficial in various disciplines of modern client/server applications but at other side, several massive vulnerabilities have been directly/in-directly associated with them. To resolve the security issues, a security mechanism is proposed which hide the sensitive information of images before transmitting to networks. Random size image samples have used and encrypted to protect them from unauthorized entities. The encryption mechanism manipulates the sample images, and corresponding secret codes are generated which help to protect the images from adversaries. To provide an indestructible security mechanism, cryptography algorithms are deployed and considered as best solutions to keep the secret information of images.*

***Keywords:*** *Local Area Network/Wide Area Network, Images Hiding, Security mechanisms, Secret codes, Security issues.*

## 1. INTRODUCTION

In past, the computer systems were used as standalone systems or may connect with peripheral devices. As passage of time, personal based computer networks are introduced that shared the information in limited area (i.e., small type of LAN) between limited number of computers or/and peripheral devices. In current modern age, number of networks such as LAN, WAN, WLAN, PAN, MAN and others are designed and employed to shared the information by the mean of computers and other electronic devices [1], [2] The information exchanging is a most important part of human daily life, number of electronic devices such as laptops, desktops,

Manuscript Received: Nov. 13, 2015/ Revised: Nov. 26, 2015/ Accepted: Jan 15, 2016
+ Corresponding Author: orange1469@naver.com
Tel: +82-63-270-3993, Fax: +82-63-270-2394
Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, Chon Buk National University

tablets, mobile devices and other are employed in sharing or/and in exchanging of information and the information is may in the forms of text, images, audio/video and other multimedia formats. With the revolution of internet technology, the daily information exchange is more easily and required few seconds to transmitted the information from one part of world to other part of the world; but there have been number of security issues are accounted that interrupting the information in transmission[2-5]. As a result, information does not deliverable to the destination. This research paper focuses on the common security issues that are residing in transmission of images and then employed various cryptography solutions to secure them from authorized entities.

The massive enhancement has been accounted in arena of digital content processing and manipulation; these contents may required to deliver in efficient and more reliable ways by employing of advance network infrastructures therefore, the traditional security mechanisms are no longer considered. In advance digital media, several security contents are needed such as access control, authorization and authentication and verification to handle the security risks that residing in transmission of digital images, and videos. To handle the security and privacy issues, a survey [17-21] has been conducted in which numbers of mechanisms (or techniques) are applied to overcome these issues in transmission of digital images, audio/video and information delivery. As a result, encryption based security techniques are considered as appropriate techniques to hide the sensitive information while travelling over unsecured networks or over internet [5-10], [13-16].

Therefore why? The use of cryptography techniques such asymmetric encryption and symmetric encryption are increasing day by day in secure processing of images, video and other sensitive information contents [5], [7-11], [13-16].

The research [6] by Puech et.al., indentified two dimensions to deploy of cryptography techniques during processing of digital images and videos. In first dimension, the information needs to keep secured form outside entities (or attackers) that may involve in processing. For example, the sensitive contents of paid video services are required to protect from outside attackers by employed end-to-end cryptography techniques, at the other side, there is also required to protect the sensitive contents information from paid users that restrict them from further unauthorized distribution to other users. Similar cases happen and as a result, number of threads exists in biometric system, if biometric information in the forms of faces detection and figure printers are collected from outsiders, or attackers interrupt the sensitive biometric information and employ for his/her personal benefits [6], [12].

In second dimension, the uses and deploying of cryptography techniques are classified. Several commercial cryptography tools are used (e.g., as add-ons") that provide general security protection in processing of images and video, and intended as reliable tools in defensive of security issues (or risks). In other solutions, the multimedia contents such images and video are manipulated with processing algorithms and security is embedded or account as a part of processing algorithms. This is good approach that mergers the security via cryptography techniques in, or as part of sensitive information therefore, Information (e.g., text, digital images and digital videos) would be protected against adversaries [6], [11].

## 2. PROPOSED METHODOLOGY

To secure the images from potential network adversaries such as man-in-the-middle attack, eavesdropping, image information modification and detection and others, cryptography based indestructible security solution has proposed in which random size images are accounted as sample images with distinct resolutions and security is deployed before transmitting to network and after receiving at destination.

To compute the better performance results, predominated cryptography algorithms such as RSA algorithm,

AES algorithm and hashing algorithm are deployed to secure the sensitive information of images. The selected cryptography algorithms have several advantages and disadvantages while comparing with each others. The security protection that provided by RSA algorithm is better than AES algorithm because RSA private key is unique and kept secured at both sides of transmission, but AES secret is shared between recipients or may be unsecured and breakable in transmission[1-5]. At other side, AES algorithm manipulation time is much faster than RSA algorithm processing time thus, RSA algorithm is not consider feasible for low bandwidth network(s). Whereas, hashing algorithm is employed to verify the image information contents, if may be or may be not changed in transmission. Fixed bytes code (or short code) is generated by hashing function that travels along image in transmission; at destination, image hash digest is computed and compared with sender hash digest value. Hash function provides protection against integrity attacks.

The below is the scenarios in which cryptography algorithms are deployed to secure the sensitive information of images.

I. Scenario A: Secret key is employed and shared between sender node and receive node. Secret key is generated from AES algorithm that provides authentication and confidentiality security services, and protection against attacks.

II. Scenario B: RSA algorithm is employed to enhance the security of sensitive information of images. Each node contains one key pair such as private key and public key, image encryption is performed by employing private key of sender and public key of receiver while decryption is performed by employing private key of receiver and public key of sender. RSA algorithm provides security services such as authentication and confidentiality and non-repudiation security by employing of digital signature.

III. Scenario C: Hashing algorithm is employed that generates fixed sized secure code (or hash digest) of image that is being transmitted to receiver side. This secure code is transmitted with original image to destination. At receiver side, again hash digest is computed bases on original image information and then, compared with sender hash digest. In case, sender /receiver hash digest are matched then image is accepted and receiver concludes that image has been transmitted from authorized node (sender) otherwise, image is rejected.

More detail related with each scenario is illustrated in figure1.

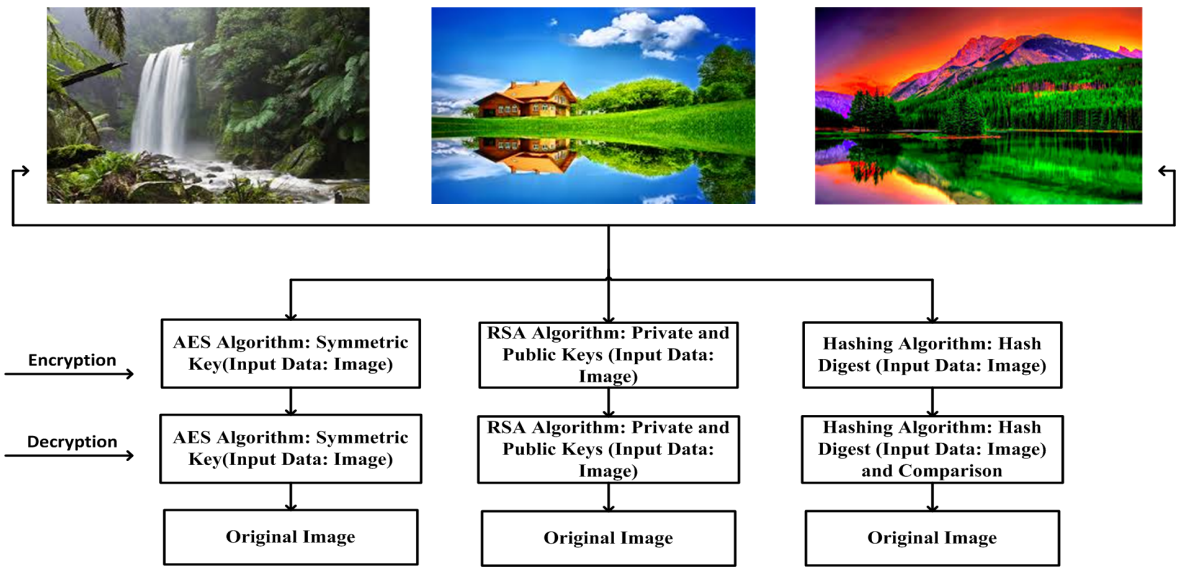


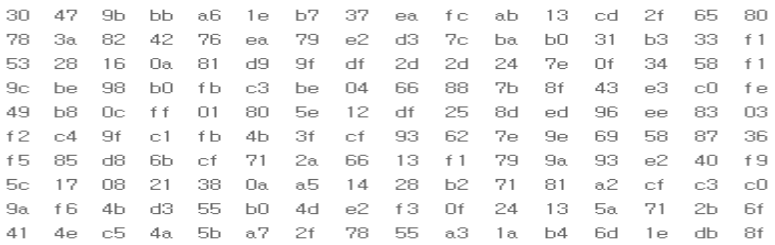

**Figure 1. Security Development Scenarios**

## 3. MEASUREMENT AND DISCUSSION

To achieve the study goals, three predominated cryptography algorithms including RSA algorithm, AES algorithm and SHA-2 hashing algorithm, are deployed in C# programming tool and tested separately to conclude the better performance results among them. Variable size images are used, and several times have been transmitted between recipients; the best and appropriate performance results are computed and depicted in table 1 according to our knowledge.

In network setup, numbers of nodes (or systems) are configured and connected with each other, using bandwidth of 5Mbps. However, nodes limit is not defined because the traffic has been carried in unicasting transmission. Each time, image is selected and security is deployed before transmitting to receiver side.

In scenario A, symmetric encryption using AES algorithm is deployed on selected image and transmitted to receiver side. Upon, receiving, shared secret key is employed to decrypts the image. The secret key is shared between recipients via secure link, and distributed statically that eliminates the uses of certificate authority (CA). At both sides, single shared key has been used, which minimizes the session during key generation and algorithm computation. The below screen shot illustrated the bytes in hexadecimal format, which computed after deploying of AES algorithm.




To examine shared secret key and its secure distribution, key creaking tool is employed during transmitting of image between recipients. As consequence, two time attacks are useful, but attack impact is low that does not effects the secret key. Meaning that, the encrypted image is secured against adversary during transmission.

**Table 1. Performance results**

| No. | Original Image Size | AES Encryption Time(ms) | RSA Encryption Time(ms) | Hashing (SHA-2) Time(ms) | Security Test |
|---|---|---|---|---|---|
| 1. | 858 KB | 8900ms | 55000 ms | 39000 ms | Verified |
| 2. | 826 KB | 8500 ms | 53000 ms | 37000 ms | Verified |
| 3. | 581 KB | 5700 ms | 33200 ms | 24000 ms | Verified |
| 4. | 757 KB | 7500 ms | 46700 ms | 31000 ms | Verified |
| 5. | 762 KB | 7600 ms | 48300 ms | 34000 ms | Verified |
| 6. | 548 KB | 5500 ms | 31700 ms | 22000 ms | Verified |
| 7. | 759 KB | 7500 ms | 47000 ms | 32000/32sec | Verified |
| 8. | 606 KB | 6700 ms | 35700 ms | 26000 ms | Verified |
| 9. | 65.0 KB | 2100 ms | 7300 ms | 1000 ms | Verified |
| 10. | 60.2 KB | 1900 ms | 7200 ms | 900 ms | Verified |

In scenario B, asymmetric security solution (using RSA algorithm) is deployed on selected image before transmitting to open network (or receiver side). RSA security computation is differing for AES algorithms; two keys such as public and private keys are employed during image encryption and decryption. In proposed

security deployment, RSA keys are generated and also distributed statistically among nodes that eliminate the uses of certificate authority (CA).

Each node contains key pair to deploys the security on selected image such that, sender keeps his/her private key and receiver public key and receiver keeps his/her private key and sender public key. The private keys are only known by sender and receiver therefore, RSA security development is accounted better and secured while comparing with AES algorithm. The below screen shot illustrated the bytes in hexadecimal format, which computed after deploying of RSA algorithm.

```
0x74 0x9d 0xec 0xab 0x7e 0xe5 0x1f 0xf 0xc9 0x1b 0xf2 0x99 0xe2 0xd4 0x73 0x75
0x7a 0xe1 0xe3 0x5f 0xae 0xe0 0x5c 0xa8 0x1b 0xee 0xd7 0x75 0x6d 0x3f 0x40 0x98
0xf1 0xef 0x98 0xd5 0xe3 0xab 0x2f 0x79 0x49 0x5a 0x68 0x70 0xf4 0xbe 0xd5 0xe9
0x35 0xfa 0xc7 0xdb 0xe1 0x3d 0x10 0x56 0x65 0xf5 0xa1 0x96 0xc0 0x9b 0x80 0xb2
0x40 0xf2 0x37 0x68 0x88 0x50 0x6a 0xf8 0xfb 0x4d 0xe8 0xcd 0x72 0x95 0x56 0xe7
0xca 0x6 0x73 0xe0 0x96 0xcc 0x80 0xee 0x9a 0x96 0x20 0x90 0xc1 0x58 0x15 0xce
0xd3 0x39 0xc9 0x30 0x30 0x7c 0x1 0x2 0xae 0x19 0x8 0x31 0x12 0xaf 0xbb 0x9e 0xf3
0x1e 0xfd 0xd2 0x49 0xc9 0x80 0x2f 0x98 0xa9 0x94 0x8a 0x7a 0x5f 0x92 0xa6
```

To evaluate the proposed security implementation (using RSA algorithm), eavesdropping and man-in-the-middle attacks have accounted using tools such as ethereal and ethercap and system behavior is tested during attacking scenario. The attacks are launches number of times to intercept the normal flow of traffic, but in our case, we do not successful to capture, the images during abnormal transmission. However, non–repudiation security service is a limitation of RSA algorithm, but would be achieved by digital signature algorithm.

In scenario C, fixed size secure code is generated using SHA-2 hashing algorithm and transmitted with selected image. Upon receiving, hash digest is computed and compared with sender hash value for verification purposes. By comparing the sender/receiver hash digests, the selected images are secured against potential attacks such as image modification, image deletion and image reply. In-case, there are still chances of security threads then RSA private key is employed on computed hash digest, which provides the non–repudiation security for selected images.

```
hex: 010f60d2927a35d0235490136ef9f4953b7ee453073794bcaf153d20a64544ea
HEX: 010F60D2927A35D0235490136EF9F4953B7EE453073794BCAF153D20A64544EA
```

As consequence, asymmetric encryption is better than symmetric encryption in terms of security computation, but usually required much time in processing while comparing with symmetric encryption. At other side, digital signature algorithm provides strong security (i.e., on–repudiation security service) by deploying of RSA and SHA-2 algorithms, but also requiring much time during computation.t

## 4. CONCLUSION AND FUTURE WORK

By replacing the existing technology with new developments of current age, several limitations have been removed due to enhancements made in arenas of information technology (IT) and computer technology. In computer networks, several local area networks (LANs) are connected together to make a wide area network (WAN) and many WANs are connected which configured the whole world as a local hub of information exchanges. However, to transmits or exchanges the information within secure channels is still to be considered as limitations of modern networks. Therefore, current research has deployed cryptography based security mechanisms which kept secured the sensitive information, as in the form of images. Several times random size images in the forms of secret codes are transmitted between nodes in network and security is tested. The

computed results show that significant enhancements are accounted during image exchanging between nodes in in-secured network setup. In future work, panorama images would be selected and transmitted in secure channels and security would also be considered by employing various techniques, with performance comparison.

## ACKNOWLDEGEMENT

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] Panicker, O.A.; Jabeenaa, A.; Hassan Mujeebb, A., "Advanced image encryption and decryption using sandwich phase diffuser and false image along with cryptographical enhancement," Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on , vol., no., pp.833,837, 2010, doi: 10.1109/ICUMT.2010.5676538

[2] Chao-Shen Chen; Rong-Jian Chen, "Image Encryption and Decryption Using SCAN Methodology," Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on , vol., no., pp.61,66, 2006, doi: 10.1109/PDCAT.2006.71

[3] R.; Johar, A.; Soni, V., "An Encryption and Decryption Algorithm for Image Based on DNA," Communication Systems and Network Technologies (CSNT), 2013 International Conference on , vol., no., pp.478,481, 2013, doi: 10.1109/CSNT.2013.105

[4] Yunpeng Zhang; Fei Zuo; Zhengjun Zhai; Cai Xiaobin, "A New Image Encryption Algorithm Based on Multiple Chaos System", International Symposium on Electronic Commerce and Security, 347-350, 2008

[5] M. Singh, et al., "Encryption and decryption using a sandwich phase diffuser made by using two speckle patterns and placed in the Fourier plane: Simulation results", Opt. Int. J. Light Electron. Opt. 2008doi:10.1016/j.ijleo.2008.03.025

[6] Madan Singh; Arvind Kumar; 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, 2009

[7] Hongjuan Liu; Zhiliang Zhu; Huiyan Jiang; Beilei Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map", The 9th International Conference for Young Computer Scientists, 3016- 3021, 2009

[8] 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, Article ID 738687..

[9] K. Sakthidasan; B. V. Santhosh Krishna,” A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images,” International Journal of Information and Education Technology, Vol. 1, No. 2, 2011

[10] Musheer Ahmad; M. Shamsher Alam, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping,” /International Journal on Computer Science and Engineering, Vol.2 (1), 46-50, 2009

[11] Ling Wang; Qun Ye; Yaoqiang Xiao et aI, "An Image Encryption Scheme Based on Cross Chaotic Map", 2008 Congress on Image and Signal Processing, 22-26, 2008

[12] Xu Shu-Jiang; Wang Ying-Long; Wang Ji-Zhi; Tian Min, "A Novel mage Encryption Scheme Based on Chaotic Maps", 2008, ICSP.9th International Conference on Signal Processing, 1014-1018, 2008

[13] Lu Ming-Xin; Lai Xue-Jia; Xiao Guo-Zhen; Qin Lei., "Symmetric Key Cryptosystem with DNA Technology Department of Information Management", Cancer Research Institute, Queen's University, Kingston, Canada, 2001.

[14] Sherif T. Amin; Magdy Saeb; Salah El-Gindi, "A DNA-based Implementation of YAEA Encryption Algorithm, " IASTED International Conference on Computational Intelligence (CI 2006), San Francisco, 2006.

[15] Jui-Cheng; Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption," Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on , vol.4, no., pp.49,52 vol.4, 2000, doi: 10.1109/ISCAS.2000.858685

[16] J. Fridrich, "Image Encryption Based on Chaotic Maps", IEEE International Conference on Systems, Man, and Cybernetics, Computaional Cybernetics and Simulations, pp.1105 -1110, 1997

[17] Kumar, M.R.; Linslal, C.L.; Pillai, V.P.M.; Krishna, S.S., "Color image encryption and decryption based on jigsaw transform employed at the input plane of a double random phase encoding system," Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on , vol., no., pp.860,862, 2010, doi: 10.1109/ICUMT.2010.5676474

[18] Shahzad, A.; Lee, M.; Lee, Y.-K.; Kim, S.; Xiong, N.; Choi, J.-Y.; Cho, Y. "Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information," Symmetry, 2015, 7, 1176-1210

[19] Sharma; Devesh Mishra; Ankur Agarwal., "Efficient image encryption and decryption using discrete wavelet transform and fractional Fourier transform," In Proceedings of the Fifth International Conference on Security of Information and Networks (SIN '12). ACM, New York, NY, USA, 153-157, 2012, doi:10.1145/2388576.2388598

[20] El Sawda, R.; Al Falou, A.; Keryer, G.; Assoum, A., "Image Encryption and Decryption by Means of an Optical Phase Mask," Information and Communication Technologies, 2006. ICTTA '06. 2nd , vol.1, no., pp.1474,1477, 0-0 0, doi: 10.1109/ICTTA.2006.1684599

[21] Chao-Shen Chen ;Rong-Jian Chen, "Image Encryption and Decryption Using SCAN Methodology," In Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '06). IEEE Computer Society, Washington, DC, USA, 61-66, doi:10.1109/PDCAT.2006.71