IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 2, February 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Securing Medical Images Transmitted via Internet Using RSA Algorithm

Aimable Munezero1, Dr. Cheruiyot W.K2, Dr. Kimani3

Abstract

Applying security to medical images is important to protect the privacy of patients' information. It is a great challenge for medical institutions to maintain patients' privacy. Unauthorized access may result, either to an illegal use or to the disclosure of patients' information. This study is aimed secure medical images exchanged between doctors and physicians using R. Rivest, A. Shamir, and L. Adleman (RSA) algorithm. To secure images requires cryptography, and RSA algorithm to achieve confidentiality, and data integrity. Improving cryptography part needs to use an encryption algorithm that stands for a long time against different attacks. Indeed, a key model for storage, retrieval and authentication of data in the encrypted medical image database is used. A transparent method for the output of images from the database through the doctor is provided

And to have an original image, decryption is the only way to succeed. All data have to be transferred encrypted among users using by a common key model that enables two parts to secure images, through encryption and decryption techniques.

1. Introduction

Until recently, the sole responsibility of keeping patients' records in confidence was with the physicians. This meant that the physician was not to disclose any medical information revealed by a patient or discovered by a physician in connection with the treatment of a patient to any unauthorized person. (A. Mahmood, Obimbo, Hamed, & Dony, 2013) However, with the advent of recent computer technology, and it's permeation into the medical field through E-health, Telemedicine (Saylor, 2013) to name but a few, the challenges of confidentiality arising from the storage and transmission of medical data cannot be left to physicians alone. Indeed, transferring medical data such as radiological results from a medical database center to another one without applying security techniques means low level of privacy for patients. Medical information transmission has increased with the use of telemedicine. Telemedicine is important because it enables consultations by remote specialists, loss-free and immediate availability of individual patient information, and improved communication between partners in health care sector (Wang, Geng, Fan, & Feng, 2008).

(Chang, Hwang, & Chen, 2001). A major issue of computer networks is to prevent important information from being disclosed to illegal users. For this reason, encryption techniques were introduced. Most encryption techniques have an easy implementation and are widely used in the field of information security. During the last decade, the use of the computer networks has grown spectacularly, and this growth continues unabated. Almost all networks are being installed, interconnected, and connected to the global internet. The internet is commonly seen as the first incarnation of an information superhighway. Today more and more information has been transmitted over the internet. Information is not only text but also audio, image, and other multimedia. Images have been widely used in our daily life. However, the more extensively we use images the more important their security will be. For example, it is important to protect the diagrams of army emplacements, the diagram of bank building construction and important data captured by military satellites.

In addition, the number of computer crimes has increased recently. Images security has become an important topic in the current computer world. Most tradition or modern cryptosystems have been designed to protect textual data (Denning, 1982). An original important and confidential plaintext is converted into ciphertext that is apparently random non-sense. Once the ciphertext has been produced, it is saved in storage or transmitted over the network. Upon reception, the ciphertext can be transformed back into original plaintext by using decryption algorithm. However, images are different from text.

Digital images are usually represented as two-dimensional (2D) arrays. For protecting the storage 2D data, this must be converted to one-dimension (1D) arrays before using encryption techniques.

1. RSA security protocol

The RSA algorithm involves three steps: key generation, encryption and decryption.

a) Key generation

RSA involves a public key and a private key**.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key which is known to the user only (Paar & Pelzl, 2009). The keys for the RSA algorithm are generated the following way (Stallings, 2006):

i. Select random prime numbers p and q, and check that p! = q for security purposes, the integers p and q should be chosen uniformly at random and should be of similar bit length. Prime integers can be efficiently found using a primality test.

ii. Compute modulus $n = pq$ is used as the modulus for both the public and private keys.

iii. Compute phi, $\varphi(pq) = (p-1)(q-1)$

iv. Choose an integer e such that 1 < e < φ(pq), and e and φ(pq) share no divisors other than 1 i.e., e and φ(pq) are co-prime (gcd(e, φ) = 1) e is released as the public key exponent e having a short bit-length and small Hamming weight results in more efficient encryption. However, small values of e (such as e = 3) have been shown to be less secure in some settings.

v. Determine d (using modular arithmetic) which satisfies the congruence Relation de=1 (mod φ(pq)) or d = **e-1** mod φ or we can say differently, ed − 1 can be evenly divided by the totient (p − 1)(q − 1).

b) Encryption

Receiver transmits his/her public key (n,e) to sender and keeps the private key secret. Sender then wishes to send message **M** to receiver. He first turns **M** into an integer 0 < m < n by using an agreed-upon reversible protocol known as a padding scheme. He/she then computes the ciphertext c corresponding to: c=me mod n. This can be done quickly using the method of exponentiation by squaring.

c) Decryption

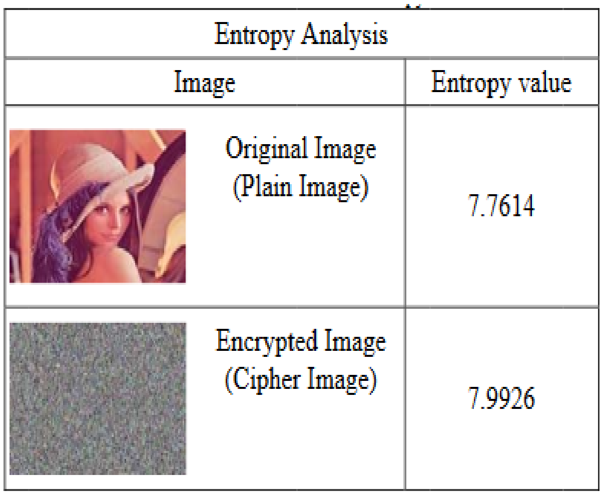
Receiver can recover m from c by using his/her private key exponent d by the following computation: m=cd mod n given m, she can recover the original message **M** by reversing the padding scheme.

2. Securing images related works

a. Block-Based on Shifted encryption and decryption

According to the differences between images and text, recently there have been several techniques to encrypt and decrypt them. (Kamali, Shakerian, Hedayati, & Rahmani, 2010) presented a modification to the Advanced Encryption Standard (MAES) to provide a high level security and better image encryption. The result shown by them was higher than that of original AES encryption algorithm.

(Younes & Jantan, 2011) introduced a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, and using the transformation algorithm it was rearranged, and then the Blowfish algorithm is used for encrypting the transformed image. Their results showed that the correlation between image elements was significantly decreased. Their results also showed that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.



Entropy Analysis		
Image		Entropy value
	Original Image (Plain Image)	7.7614
	Encrypted Image (Cipher Image)	7.9926

Figure 1: Block-Based on Shifted encryption and decryption

b. Chaos Encryption Algorithm using Key Generation from Biometric Images

(Ismail, Amin, & Diab, 2010) proposed chaos-based stream cipher, composing two chaotic logistic maps and external secret key for encryption of image. In this an external secret key of 104 bit and two chaotic logistic maps are used to differentiate between the encrypted image and the plain image. Further, the secret key is modified after encrypting of each pixel of the plain image which makes the encrypted image more robust. Then there is a feedback mechanism which increases the robustness of the proposed system.

Indeed, several chaos based ciphers have been suggested in the last decade. Some of them exploit 1-D chaotic systems for generating the required secret keys (Fu, Ch., Zhang, Z., Chen, Z.,and Wang, X., 2007). After generating the key, the image pixels are then shuffled and modified according to the obtained key. On the other hand, some encryption algorithms depend on two-dimensional maps to directly handle the digital image which is represented as 2D array of pixels (Zhai, Y., Lin, S., Zhang, and Q, 2008). Similarly, chaotic based ciphers are sender and receiver to obtain the encrypted and the decrypted image, respectively. First, a secret biometric image is exploited by the sender/receiver to generate the secret key.

The encryption operations are applied to the plain image to get the cipher image. The structure of the proposed cipher relies on a data-dependent feedback mechanism in which the encipher of each pixel is made dependent on the encryption properties of the previous cipher pixel, which in turn, makes the cryptosystem robust against any type of attacks. The following subsections present the three phases of the proposed algorithm.

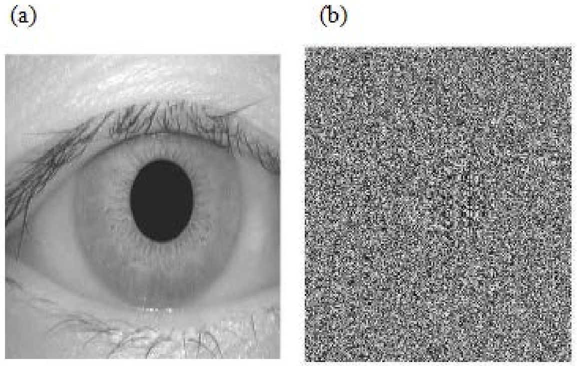


Figure 2: Encryption results for chaos algorithm (from Ismail, Amin, & Diab, 2010)

c. Distribution of pixels of image

It shows that Histograms of several cipher images and their corresponding plain images having widely different contents and sizes have been analyzed. One example of histogram analysis for well-known image 'Lena' is shown in Figure 2. Histograms of red, blue and green components of image (Figure 2(a)) are shown in Frames (b), (c) and (d) respectively. In Frames (f), (g) and (h) respectively, the histograms of red, blue and green components of the cipher image (Figure 2(e)) are shown. Comparing the histograms, it is found that encryption process returns noisy images.

Histograms of cipher images, approximated by uniform distribution, are quite different from that of the plain image and contain no statistical resemblance to the plain image. This is consistent with the perfect security defined by Narendra K Pareek [2012] and the proposed encryption scheme resists against the known-plaintext attack.

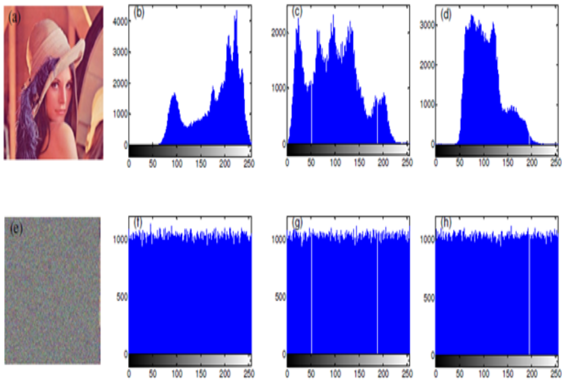


Figure 3: Histograms corresponding to RGB components of plain image ‘Lena’ and its corresponding cipher image

3. Performance measures

This section discusses the performance analysis of the SMIT using RSA, based on time consumption and simulation results compared to the related works (Borda, 2011). We evaluate the time for encryption, decryption and key generation.

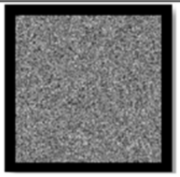
The efficiency comparison between SMIT using RSA and other related works are given in Table 4.1 and Table 4.2. The comparison is based on the data provided in (Borda, 2011) where based on the simulation results 0.295829 Sec.; 56.385263Sec. And 0.295829 Sec is used by DES while 7.201574 Sec, 126.305795 Sec. and 110.416216 Sec. are used by Blowfish for key generation, encryption and decryption respectively. Our scheme is more efficient since it uses only 0.11Sec., 0.245 Sec. and 30 Sec. for key generation, encryption and decryption respectively.

Based on the protocol design, our scheme better than DES and Blowfish (Borda, 2011) since the above protocol requires the communicating parties (sender and receiver) to share a secret key, which means that they should meet in advance before exchanging any information. However, our protocol uses RSA which an asymmetric cryptosystem where the sender and receiver does not need to meet in advance since each has a pair of keys namely private and public key. The public key is published and known to every one while the private key is kept securely and know only to the owner.

Table 1: Efficiency comparison

	Key generation Time (Sec)	**Encryption Time** (Sec)	**Decryption Time** (Sec)	**Protocol**
DES (Borda, 2011)	0.29	56.38	63.39	Symmetric
Blowfish (Borda, 2011)	7.20	126.30	110.41	Symmetric
SMIT using RSA	0.11	0.24	30	Asymmetric

Based on the simulation results presented in Table 4.1, the SMIT using RSA it is more secure compared to DES and Blowfish where after encryption the cipher text looks like an image; this can facilitate the adversary to guess the plain text and then launches a chosen cipher text attack. In the SMIT using RSA after encryption the adversary cannot guess what the plain text was since the cipher text looks like random number then the attacker cannot decrypt the plain text.

	Simulation result after Encryption
Blowfish (Borda, 2011)	

SMIT using RSA	73084248588051601835690 43
	790479931236665835812190 5
	429861459014096364623990 3
	329032478608956602164659 8
	742952146088479957194346 4
	799697856857842024600954 0

Table 2: Simulation results of security level

Table 4.2 demonstrates the comparison between the SMIT using RSA, Blowfish. The SMIT using RSA converts image into random number and it is more secured (Ali & Adnen, 2012) during transmision because the encrypted image is represented as random numbers. Hence hackers cannot discover or guess the plain text.

Previous techniques the number of images retrieved were five using blowfish security level, was 66.02% then after introducing new technique which is SMIT using RSA The percentage security increased from 66.02% to 94.52% that shows the effectiveness of new technique.

Table 3: Security level comparison

Original images	**Decrypted using Blowfish**	**Decrypted using SMIT**
1	70	95
2	68.8	93.7
3	69.3	91
4	63	96
5	59	96.9
AVG	66.02	94.52

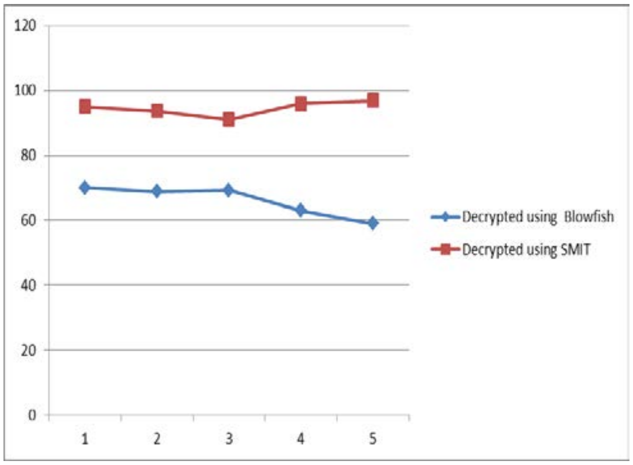
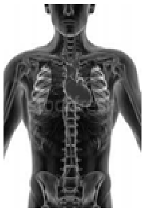
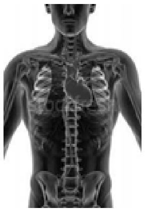


Figure 4: Security level for retrieved medical image using diagram

This is medical image after transformation within random numbers or after encryption. Encryption is a process which uses a finite set of instruction called an algorithm to convert original medical image, known as plaintext, into random number, known as cipher text, its encrypted form. Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data. With the help of key and the algorithm we can encrypt or Decrypt the image plaintext into cipher text and then cipher text back into plaintext.

Table 4: Comparison of original and encrypted image

Original Image	Encrypted Image	Decryption Image
	457800997615 679990805332 703721125729 989429908671 260132574438 720349617342	

4. Conclusion

In this research, implemented an algorithm "SMIT" using RSA, which can be used to achieve privacy of medical image transmitted over the Internet. The SMIT is based on the RSA cryptosystem which is used by the sender to encrypt a medical image before transmission and by the receiver to decrypt the image at the reception side.

The SMIT using RSA achieves privacy, confidentiality and integrity of medical image; also it is more secure 94.52% because using Simulation result after Encryption since it converts the encrypted image into random numbers which cannot be predicted to the adversary. The SMIT using RSA is more efficient in terms of time consumption since it uses less time for encryption and decryption of medical images where uses 0.11 sec during keys generation, 0.245 sec during encryption and 30 sec during decryption.

5. References

1. Ali, S., & Adnen, C. (2012). RSA algorithm implementation for ciphering medical imaging. *IJCER, 1*(2), 44-49.
2. Alsafasfeh, Q. H., & Arfoa, A. A. (2011). Image encryption based on the general approach for multiple chaotic systems. *Journal of Intelligent Learning Systems and Applications, 3*(3), 198.
3. Bani Younes, M. A., & Jantan, A. (2008). Image encrytion using block based transformation algorithm.
4. Borda, M. (2011). Statistical and Informational Model of an ITS *Fundamentals in Information Theory and Coding* (pp. 7-52): Springer.
5. Chang, C.-C., Hwang, M.-S., & Chen, T.-S. (2001). A new encryption algorithm for image cryptosystems. *Journal of Systems and Software, 58*(2), 83-91.
6. Delahaye, J.-P. (2000). La cryptographie RSA vingt ans après. *Pour la science, 267*, 104-108.
7. Denning, D. E. (1982). Cryptography and data security.
8. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory, 22*(6), 644-654.
9. Hassan, M. A. S., & Abuhaiba, I. S. I. (2011). Image encryption using differential evolution approach in frequency domain. *arXiv preprint arXiv:1103.5783*.
10. Indrakanti, S. P., & Avadhani, P. (2011). Permutation based image encryption technique. *International Journal of Computer Applications (0975–8887) Volume*.
11. Ismail, I. A., Amin, M., & Diab, H. (2010). A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps. *IJ Network Security, 11*(1), 1-10.
12. Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. (2010). *A new modified version of advanced encryption standard based algorithm for image encryption.* Paper presented at the Electronics and Information Engineering (ICEIE), 2010 International Conference On.
13. Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography*: CRC press.

14. Kolhekar, M., & Jadhav, A. (2011). Implementation of elliptic curve cryptography on text and image. *International Journal of Enterprise Computing and Business Systems, 1*(2).
15. Mahmood, A., Obimbo, C., Hamed, T., & Dony, R. (2013). Improving the Security of the Medical Images. *International Journal of Advanced Computer Science and Applications, 4*(9), 137-146.
16. Mahmood, A. B., & Dony, R. D. (2011). *Segmentation based encryption method for medical images.* Paper presented at the Internet Technology and Secured Transactions (ICITST), 2011 International Conference for.
17. Nag, A., Singh, J. P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D., & Sarkar, P. P. (2011). *Image encryption using affine transform and XOR operation.* Paper presented at the Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on.
18. Niederreiter, H. (2002). *Coding theory and cryptology* (Vol. 1): World Scientific.
19. Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*: Springer Science & Business Media.
20. Pandey, U., Manoria, M., & Jain, J. (2012). A novel approach for image encryption by new M box encryption algorithm using block based transformation along with shuffle operation. *International Journal of Computer Applications, 42*(1), 9-15.
21. Qaid, G. R., & Talbar, S. N. (2012). Encryption and Decryption of Digital Image Using Color Signal. *IJCSI International Journal of Computer Science Issues, 9*(2), 588-592.
22. Rhee, M. Y. (2003). *Internet security: cryptographic principles, algorithms and protocols*: John Wiley & Sons.
23. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems.

Communications of the ACM, 21(2), 120-126.

24. Rohini, S., & Bairagi, V. (2010). Lossless medical image security. *International journal of applied engineering research, 1*(3), 536.
25. Saylor, M. (2013). *The mobile wave: how mobile intelligence will change everything*: Vanguard Press.
26. Seyedzade, S. M., Mirzakuchaki, S., & Atani, R. E. (2010). *A novel image encryption algorithm based on hash function.* Paper presented at the 2010 6th Iranian Conference on Machine Vision and Image Processing.
27. Simmons, G. J. (1979). Symmetric and asymmetric encryption. *ACM Computing Surveys (CSUR), 11*(4), 305-330.
28. Stallings, W. (2006). *Cryptography and network security: principles and practices*: Pearson Education India.
29. Tahmoush, D., & Samet, H. (2007). *A new database for medical images and information.* Paper presented at the Medical Imaging.
30. Wang, Y.-Z., Geng, S.-C., Fan, Y.-J., & Feng, Z.-Q. (2008). *Research the Compression and Transmission Technology of Medical Image Base on the Remote Consultation.* Paper presented at the 2008 2nd International Conference on Bioinformatics and Biomedical Engineering.
31. Yao, A. C. (1982). *Theory and application of trapdoor functions.* Paper presented at the Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on.
32. Ye, C., Xiong, Z., Ding, Y., Zhang, X., Wang, G., & Xu, F. (2015). Joint fingerprinting/encryption for medical image security. *International Journal of Security and Its Applications, 9*(1), 409-418.
33. Younes, M. B., & Jantan, A. (2011). *Image Encryption Using Block-Based Transformation Algorithm: Image Encryption and Decryption Process Using Block-Based Transformation Algorithm*: LAP Lambert Academic Publishing.