CURRENT RESEARCH IN
COMPUTER SCIENCE
ISSN 2788-7707
MAY. 2021 VOL. 1, NO. 1

Study on Data Confidentiality in Telemedicine Practice

Ganiyu Arowolo and Lambe Jennifer
Department of Mathematics and Computer Science, Ritman University, Ikot Ekpene, Nigeria

ABSTRACT

The study examines the security threat to the practice of telemedicine and proffers a solution through the integration of the RSA cryptography and the F4 frequency domain steganography. The integration of the two techniques results in computational complexity but the cost of this when compared to that of security of data makes the later worth the while. It is difficult to differentiate the digital image object from the stego image object with the human eyes. One of the limitations seen in the approach is the low carrying capacity due the F4 algorithm employed in the study. F4 uses the Discrete Cosine Transform that limits the information captured by both the patient and the physician. The RSA cipher provides asymmetry key that ensures a better security than the F4 which operates without a key. So the combination of both the F4 and RSA complements each other. While RSA ensures the provision of asymmetry key, the F4 ensures the concealment of the information from an intruder. Medical data are critical data that its concealment from unauthorized recipient is very important. Confidentiality of data is a key component to the practice of telemedicine and its lack has tended to discourage potential patients from such a platform. Once a patient discovers that the confidential information he had provided to a machine has been intruded on by an unknown person he is likely to withdraw his patronage from such a system. Though he could be vexed by the slow speed of processing but this could be tolerated. Further study of embedding the message in a looseless image is however suggested to handle the complexity of processing and improve on the carrying capacity of the stego image.

KEYWORDS

RSA; Cryptography; Steganography; Telemedicine; F4; Security; Confidentiality; Integrity.

1. Introduction

Two main technologies of Video Teleconferencing (VTC) and Store and Forward (SF) are applied in telemedicine. In the VTC, there is a synchronous communication where data are sent and received at real time. The patient and the medical practitioner need be online at the same time. In the SF technology, data could be

sent to the medical personnel and stored for later retrieval. This could be sent via E-mail or any other electronic medium so both the patient and the medical personnel need not be online at the same time. The SF is inexpensive to implement. SF however denies the opportunity of interaction which is a core ingredient in medical practice. VTC offers the privilege of interaction but comes with additional cost. Security and privacy of data are the major challenges in both SF and VTC though this is very obvious in the SF technology.

Another major challenge of telemedicine is the dearth of enabling laws in most countries. Due to diverse culture, religion and tribe, it is becoming difficult to practice telemedicine in these countries. The reluctance and inabilities of legislatures to enact enabling laws for the practice of telemedicine border mostly on privacy and security issues. Patients lack the requisite confidence to submit themselves to be interrogated by a machine. Confidential information disclosed to a human doctor could not be divulged to a machine in the name of a doctor. This has inhibited in no small measures the practice of telemedicine especially in the developing countries. In effect, the gains of prompt treatment, low cost of consultation etc are being overshadowed by this drawback.

Security of information is concerned with a way to ensure that the source and destination of information and the integrity of the information are protected from unauthorized disclosure, alteration or destruction. One way of doing this is by keeping the information from the reach of every other person except the intended receiver (the person the information is meant for). The intended receiver must be ascertained through the process called authentication before the content of the message is disclosed to. The vulnerability of computer networks especially in a wireless medium calls for concerted efforts in ensuring that only the intended receiver gets what is meant for him as intruders nose around the network seeking for a way to 'steal' information. Sometimes they (intruders) alter information maliciously before the information gets to the authorized owner. Altering medical information portends a great danger to both the sender and the receiver. For example, if the information sent by a patient is tampered with before getting to the medical practitioner, it may lead to wrong diagnosis. That sent by a medical doctor to his patient if tampered with could as well lead to a wrong therapy.

In the light of this, it is pertinent to ensure that the medium of communication in telemedicine is secured. One way of protecting information from being tampered by an intruder is by covering such information in such a way that only the authorized user can uncover it. Another way is to present the information in a meaningless format to all except the intended authorized receiver.

The authorized receiver has the key to use in converting the purportedly 'meaningless' information to a meaningful message. The paper intends to combine the asymmetric cryptography scheme, the RSA algorithm with the F4 steganographic algorithm in order to ensure that data and information send from patients to medical personnel are securely sent and received.

In this study, the two methods are combined together to design a foolproof system of securing data and information transmitted in a telemedicine platform. The rest of the paper is organized thus; in Section 2, the literature review is presented. The design of cryptstego system which integrates the steganography algorithm and a cryptographic cipher is presented in Section 3. An experiment conducted with a simulated scenario is presented in Section 4. Conclusion of the research and recommendations made are presented in Section 5.

2. Literature

The main purpose of steganography is to hide the existence of information in a medium such as video, audio or image so that an intruder will not be aroused by the presence of such an object. According to Hussian and Hussian (2013), Images are the most popular carriers of hidden messages since human visual system cannot easily detect an image with a hidden message from the one without a hidden message. 3 main techniques are

identified for embedding information in any of the mentioned media namely; transform or frequency domain, spatial domain and masking and filtering techniques. Chikara and Kumar (2010) proposed a concealment of encrypted messages using the Discrete Cosine Transform (DCT) in JPEG images. In Jaheel et al (2015) a design and implementation of a steganography system using visible image is undertaken. Obot and George (2017) used the hide and seek algorithm to propose an information managing system in fighting terrorism. Palewar and Shende (2013) evaluated the robustness of watermarking using watermarking enhanced performance metric.

Cryptography, a method of transmitting information in a meaningless format to all except the intended receiver who has the key to unlock the message and decipher the contents has various techniques of processing. A combined approach to securing information using steganography and asymmetric cryptography is designed in Obot and Edoho (2013). In Obot (2018), practical cryptography and steganography is presented where different methods of the two information processing methods are highlighted. The Data Encryption Standard (DES) used in symmetric key encryption and the Rivest, Shamir and Adleman (RSA), an asymmetric key encryption are among the popular ciphers in cryptography.

Youm et al (2011) developed web-based health check-up systems that can asses physical and physiological measures of patients at a distance and report to a doctor. Olanrewaju et al (2017) proposed digital watermarking for tackling issues of privacy and security in telemedicine. In Abdul-Mumin and Gbolagade (2016), a new RSA encryption scheme is proposed. Akomolafe and Taiwo (2015) designed a framework for secured data sharing in the cloud with the aim of handling privacy and access control issues inherent in cloud computing. Benabdellah et al (2006) proposed encryption-compressed of still images using the FMT transformation and the DES algorithm. Obot, et al (2012) improve on the classical Playfair cipher and applied it to propose data security and integrity in a cashless society. Hassibian and Hassibian (2016), present the benefits, categories and barriers of telemedicine in developing countries.

3. Materials and Methods

A flow diagram for the CryptStego system as adapted from Obot and Edoho (2013) and modified to suit this application is shown in Figure 1.

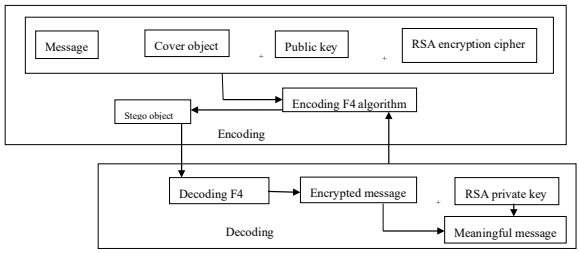

Figure 1. A flow diagram for CryptStego System

The flow diagram is a two-tier architecture comprising the encoding of message in the first layer and decoding in the second layer. The encoding process involves encrypting the message (text, audio or image) elicited from a patient using the RSA cipher which comes with a generated public key. The encrypted message is then hidden in an image file of a higher storage capacity to form a stego object. The stego object is sent to the medical personnel who decodes the file to have an encrypted message from the patient. He then uses the RSA private key to decrypt the original message to have a meaningful message to use in diagnosis. After the diagnosis, he has to encrypt his findings and therapy and encode using the F4 algorithm to send to the patient. The patient also performs decoding of what he has received from the medical personnel.

The frequency or transform domain using the F4 encoding Algorithm is presented as Algorithm 1 while the decoding algorithm is shown in Algorithm 2. Fauguer(1999). The Rivest, Shamir and Adleman (RSA) cipher is shown in Algorithm 3 Rivest, Shamir and Adleman (1978).

Algorithm1: F4 Encoding Algorithm
Encoding

1. *For i = 1,… l(m) do*
2. *P ⊚ d_i*
3. *While P = DC or P = 0, do*
4. *P = next DCT coefficient from d*
5. *Endwhile*
6. *P ⊚ absolute (P_i)*
7. *If P = m_i and P > 0 then*
8. *P ⊚ P + 1*
9. *Absolute d(d_i) ⊚ P*
10. *Else if P ≠ m_i and P < 0 then*
11. *P ⊚ P -1*
12. *Absolute (d_i) ⊚ P*
13. *Endif*
14. *If d_i = 0 Then*
15. *Next m_i = m_i*
16. *Endif*
17. *C_i ⊚ P_i*
18. *End for*
19. *Convert each 8X8 block back to spatial domain*

Algorithm 2: F4 Decoding Algorithm

1. *Convert image S to DCT domain d in 8 X 8 blocks*
2. *For i = 1, …, l(m) do*
3. *P ⊚ d_i*
4. *While P = DC or P = 0 do*
5. *P = next DCT coefficient from d*
6. *End while*
7. *P ⊚ absolute (P_i)*
8. *If P = m_i and P > 0 then*
9. *m_i ⊚ absolute (P_i) – 1*
10. *Else if P ≠ m_i and P < 0 then*
11. *m_i ⊚ absolute (P_i) + 1*
12. *Endif*
13. *Endfor*

Algorithm 3: RSA Algorithm

1. *Choose two (large) prime numbers say p and q*
2. *Compute n = p x q*
3. *Choose a number relatively prime to z and it d*
4. *Find e such that e x d = 1 mod z*
5. *Encryption begins by dividing the plaintext into blocks so that each plaintext P, falls into the interval 0<= p <= n. Encrypting message P, compute C = P^e(Mod n);*
6. *To decrypt; Compute P = C^d (mod n).*

The RSA algorithm is based on two assumptions of:

(a) There is a known fast algorithm for determining whether a given (large) number is prime
(b) There is no known fast algorithm for determining the prime factors of a given (large) non prime number.

Note that encrypting requires e and n while decrypting requires d and n. This implies that the public key consists of the pair (e,n) while the private key consists of (d,n). The inability to factorize large numbers makes the system secured.

The Experiment

We simulate a scenario where a patient sends a short note tagged 'HEART ATTACK' to a medical doctor. This is encrypted in RSA as follows. We choose small prime numbers for simplicity of the experiment and quick comprehension.

Let p = 3, q = 11 so n = 33 and z = 20. A suitable value for d (a prime number between p and q that has a common factor with z) = 7 . e can be found from 7e = 1(mod 20) = 21 = 1(mod 20) = 21/20 = 1 rem 1. Therefore, e = 3. The key to encrypt is C= Pe(mod n) = P3(mod 33). The key to decrypt is P = cd(mod n) = c7(mod 33).
So the text 'HEART ATTACK' gives the computation presented in Table 1.

Table 1. Encryption of the message 'HEART ATTACK'

Symbol	Position(P)	P^3	P^3mod(33)	Symbol	Position(P)	P^3	P^3mod(33)
HEART				ATTACK			
H	8	512	17	A	1	1	1
E	5	125	26	T	20	8000	14
A	1	1	1	T	20	8000	14
R	18	5832	14	A	1	1	1
T	20	8000	14	C	3	27	27
	27	19683	21	K	11	1331	11

Figure 2. A Digital Image

The 8 X 8 matrix block of the image in a spatial domain is as shown in Figure 3. This is transformed into a frequency domain by the F4 algorithm and the transformed matrix is shown in Figure 4. The sample of the 8 x 8 block matrix that shows the ASCII-8 equivalence of the ciphertext derived from RSA cipher hidden in the transformed image is shown in Figure 5, while Figure 6 shows the resultant image.

17	2 55	10	15 5	16 3	68	12 6	120
17	4 74	13	12 2	17 2	79	12 6	110
17	8 43	37	16 88	10 9	3	13 4	116
16	7 14 103		13 0	14 9	10 6	13 9	121
10	3 9 153		12 1	12 6	92	20 2	123
36	9 158		14 2	10 5	89	22 0	128
18	9 149		16 1	84	90	82	119
23	8 151		15 3	73	84	79	126

Figure 3. Original Image Matrix

	15						10
34	4	37	14	10	10	15	2
	16						
35	3	50	12	13	9	9	62
	10						
40	4	34	61	19	9	22	29
14						14	
1	59	10	49	16	9	2	19
14						17	
6	36	10	28	18	10	8	26
14						17	
3	41	30	11	56	10	6	62
		12	12	16		21	13
69	17	2	5	4	91	5	3
		10	13	17	13	19	12
31	59	0	5	7	8	8	4

Figure 4. Transformed Image Matrix

		1.632 1.292 0.367 0.165 0.047 0.466 0.07 0.013					
0.437		0.54 0.138 0.227 0.023				0.12 0.26 0.011	
		0.105 0.105 0.126 0.279 0.033 0.469				0.2 0.037	
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 5. Stego Matrix

Figure 6. Stego Image

4. Conclusion

The study examines the security threat to the practice of telemedicine and proffers a solution through the integration of the RSA cryptography and the F4 frequency domain steganography. The integration of the two techniques results in computational complexity but the cost of this when compared to that of security of data makes the later worth the while. It is difficult to differentiate the digital image object from the stego image object with the human eyes. One of the limitations seen in the approach is the low carrying capacity due the F4 algorithm employed in the study. F4 uses the Discrete Cosine Transform that limits the information

captured by both the patient and the physician. The RSA cipher provides asymmetry key that ensures a better security than the F4 which operates without a key. So the combination of both the F4 and RSA complements each other. While RSA ensures the provision of asymmetry key, the F4 ensures the concealment of the information from an intruder. Medical data are critical data that its concealment from unauthorized recipient is very important. Confidentiality of data is a key component to the practice of telemedicine and its lack has tended to discourage potential patients from such a platform. Once a patient discovers that the confidential information he had provided to a machine has been intruded on by an unknown person he is likely to withdraw his patronage from such a system. Though he could be vexed by the slow speed of processing but this could be tolerated. Further study of embedding the message in a looseless image is however suggested to handle the complexity of processing and improve on the carrying capacity of the stego image.

References

Abdul-Mumin S and Gbolagade (2016), A New RSA Encryption Scheme with Error Detection and Correction, The Journal of Computer Science and its Applications, 23(2): 127-136.

Akomolafe O.P., and Taiwo I. D., (2015), A Framework for Secure Data Sharing in the Cloud, The Journal of Computer Science and its Applications, 22(1): 87-93

Benabdellah M., Gharbi., Zahid N Regragui, F and Bouyakhf E (2006), Encryption-compression of still images using FMT transmission and the DES algorithm, Georgian Electronic Scientific Journal: Computer Science and Communication 4(11): 22-31

Chikara, R and Kumar S. (2010) Concealing Encrypted Messages using DCT in JPEG images, International Journal of Electronics and Electrical Engineering, 2(1)

Hassibian M. R. and Hassibian S., (2016), Telemedicine Acceptance and Implementation in Developing Countries: Benefits, Categories and Barriers, Razavi Int. Journal of Medicine' 4(3):e383382

Hussain M and Hussain M (2013), A survey of Image Steganography techniques, International Journal of Science and Technology, 54: 113-124

Jaheel H., Beiji, Z., and Jaheel A. (2015), Design and Implementation of Steganography system using Visible image, International Journal of Smart Sensing and Intelligent Systems 8(2)

Lamimnen, H., Ville, V., Keijo, R., and Hannu (2003), Telemedicine in Ophthalmology, Acta Ophthalmol Scand, 81: 105-109.

Marta, M. R., (2003), Telemedicine Payment: Then and Now. Healthcare Financial management 1:50-53

Obot O. U., George, U. D., and Udoh, S.S., (2017), Managing Information in Fighting Terrorism, Journal of the Nigerian Association of Mathematical Physics, 40: 265-272

Obot, O.U., and Edoho M. E. (2013), A Combined Approach to Securing Information using Steganography and Asymmetric Cryptography. In Conference Proceedings of the Nigeria Society of Computer Society with the theme; e-Government and National Security, 13-15

Obot, O., Ekong, V., and Okon, M., (2012), Enhanced Playfair Cryptography System for Data Security and Integrity in a cashless society, In proceedings of the Nigeria Society of Computer Society with the theme; Towards a cashless Nigeria: Tools and Strategies, 5660

Obot, O.U., (2018), Practical Cryptography and Steganography, Lambert Academy Press, Germany.

Olanrewaju R., Ali, N, Khalifa, O., Manaf A., (2013), ICT in Telemedicine: Conquering Privacy and Security Issues in Healthcare Services; Electronics Journal of Computer Science and Information Technology, 4(1): 19-24

Palewar, S. S., and Shende, R., (2013), Watermarking Robustness Evaluation using Watermarking Enhanced performance metrics, International Journal of Engineering Research and Technology 2(2)

Rivest R.L., Shamir, A., and Adleman, L (1978), A Method of obtaining Digital Signatures and Public KeyCryptosystems, CACM ,21(2)

Youm S, Lee G, Park S and Zhu W (2011), Development of Remote Healthcare System for Measuring and Promoting Healthy Lifestyle, Expert System and Applications 38(2011): 2828-2834.