Issues in Informing Science + Information Technology

An Official Publication of the Informing Science Institute InformingScience.org

IISIT.org

Volume 15, 2018

Medical Image Security using Quantum Cryptography

Olufunso Dayo Alowolodu	Federal University of Technology, Akure, Nigeria	odalowolodu@futa.edu.ng
Gabriel Kayode Adelaja	First Bank of Nigeria PLC, Lagos State, Nigeria	Gabrielkayode33@gmail.com
Boniface Kayode Alese*	Federal University of Technology, Akure, Nigeria	bkalese@futa.edu.ng
Olufunke Catherine Olayemi	Joseph Ayo Babalola University, Ikeji Arakeji, Osun State, Nigeria	ocolayemi@jabu.edu.ng

* Corresponding author

Abstract

Aim/Purpose	Medical images are very sensitive data that can be transferred to medical laboratories, professionals, and specialist for referral cases or consultation. Strict security measures must be utilized to keep these data secured in computer networks when transferred to another party. On a daily basis, unauthorized users derive ways to gain access to sensitive patient medical information.
Background	One of the best ways to which medical image could be kept secured is through the use of quantum cryptography
Methodology	Applying the principles of quantum mechanics to cryptography has led to a remarkable new dimension in secured network communication infrastructure. This enables two legitimate users to produce a shared secret random bit string, which can be used as a key in cryptographic applications, such as message encryption and authentication.
Contribution	This paper can make it possible for the healthcare and medical professions to construct cryptographic communication systems to keep patients' transferred data safe and secured.
Findings	This work has been able to provide a way for two authorized users who are in different locations to securely establish a secret network key and to detect if eavesdropping (a fraudulent or disruption in the network) has occurred

Accepting Editor: Eli Cohen │ Received: November 29, 2017 │ Revised: March 12, 2018 │ Accepted: March 26, 2018.

Cite as: Alowolodu, O. D., Adelaja, G. K., Alese, B. K., & Olayemi, O. C. (2018). Medical image security using quantum cryptography. *Issues in Informing Science and Information Technology, 15,* 57-67. https://doi.org/10.28945/4008

Recommendations for Practitioners — This security mechanism is recommended for healthcare providers and practitioners to ensure the privacy of patients' medical information.

Recommendation for Researchers — This paper opens a new chapter in secured medical records

Impact on Society — Quantum key distribution promises network security based on the fundamental laws of quantum mechanics by solving the problems of secret-key cryptography.

Future Research — The use of post-quantum cryptography can be further researched.

Keywords — medical image, quantum cryptography, security, quantum key distribution

INTRODUCTION

Medical images have become an essential part of medical diagnoses and treatments. Often, many diseases are better diagnosed through medical imaging. Occasionally, there are needs to refer patients for further diagnosis and treatment without physically moving their medical records to the referred location, and these are usually transferred through network communication infrastructure such as the internet. Usually, medical images are classified information that should be treated with utmost confidentiality. Now to ensure the integrity and confidentiality of a medical image, medical professionals must properly secure these data with the network communication infrastructure in order for the patient referred location to receive the exact transferred medical image.

Alowolodu, Alese, and Adetunmbi (2016) posit that, despite the internet providing a better solution to various kinds of scalability, flexibility, and availability, some people are still skeptical to relinquish their personal data or information over the internet.

Picture Archiving and Communications Systems (PACS) have been described as a reliable means of transferring and distributing image data. Communication of images in a PACS environment is usually over the local area network that is protected by a firewall from outside intruders (Samaan, 2016).

Nowadays, the transmission of images is a daily routine, and it is necessary to find an efficient way to transmit them over the networks. With the number of internet users on the increase every day, everything done online is under the threat of malicious intruders (Kapur, & Baregar, 2013). The transmission of images over the internet is challenging because of the high risk of eavesdroppers and internet communication hackers. In this manner, one of the secured means of transmitting the image over the internet is cryptography.

Cryptography is a security tool that provides security in the ciphers of a message. It is also the art of encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication. Cryptographic algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. Cryptography plays a central role in mobile phone communication, e-commerce, Pay-TV, sending private e-mails, and transmitting financial information, and it touches on many aspects of daily lives. There are various cryptographic schemes available, one of which is the Quantum Cryptography. Quantum Cryptography, or Quantum Key Distribution (QKD), applies fundamental laws of quantum physics to guarantee secure communication. It enables two legitimate users to produce a shared secret random bit string, which can be used as a key in cryptographic applications, such as message encryption (for instance, the one-time pad) and authentication (Van Der Walt, 2016). Unlike conventional cryptography, whose security often relies on unproven computational assumptions, QKD guarantees security based on the fundamental laws of quantum mechanics. Quantum cryptography solves the problems of secret-key cryptography by providing a way for two authorized users who are in different locations to securely establish a network secret key.

The necessity of fast and secure diagnosis is vital in the medical world to save the life of world creatures. Nowadays, the transmission of images is a daily routine, and it is necessary to find an efficient way to transmit them over networks (Lo-Varco, Puech, & Dumas, 2003; Norcen, Podesser, Pommer, Schmidt, & Uhl, 2003). For image transmission, two different approaches of technologies have been developed. The first approach is based on content protection through encryption (Berlekemp et al., 1978; McEliece 1978). In this approach, proper decryption of data requires a key. The second approach based the protection on digital watermarking or data hiding and aimed at secretly embedding a message into the data. In the current era, the transmission of images over the internet is challenging because of the high risk of eavesdroppers and unsecure communication to internet communication hackers. In this manner, the better way to transmit the image over internet is encryption.

The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either "public-key" or "secret-key" methods.

Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it (Ekert, 1995) Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. Since the encrypting and decrypting keys are different, it is not necessary to securely distribute a key. The security of public-key encryption depends on the assumed difficulty of certain mathematical operations, such as factoring extremely large prime numbers.

RELATED WORKS

Abraham and George (2015), worked on a secure image transmission technique by mosaic image using the HSV converted target image and reversible data hiding method for image protection. A secret image can be transmitted by converting it into a mosaic and hiding it inside a target image color which is further divided into smaller fragments. The proposed work established that messages sent via this method can be recovered almost without any loss. This shows that this method cannot be suitable for medical image transfer.

Kapur and Baregar (2013) used stitching and image steganography to secure an image to be sent over the network. The images are divided into parts. The first part is the encryption phase using the AES algorithm; the second part is the embedding phase where the cyphertext is embedded in into any part of the secret image to be sent. The third part is the hiding phase where steganography is performed on the output image of the embedding phase. The article written by Van Der Walt (2016) proved that an algorithm to narrow down the set of values that generated a particular set of solution could be used since most of these cryptographic algorithms depend on factoring the hardness of a large number. But the new set of quantum cryptographic algorithms depends on a more stringent test of difficulty. This is what prompted the use of quantum cryptography for this proposed work.

Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles. An important objective is to find quantum algorithms that are significantly faster than any classical algorithm solving the same problem. The premise of quantum-safe cryptography research depends on mathematical problems that are harder to break using a quantum computer. RSA and ECC cannot be used in the presence of quantum computer (Van Der Walt, 2016).

METHODOLOGY

An extensive literature review on enhanced Quantum Cryptography technique will be used to secure medical images. This will be done by true random secret key generation and eavesdropping detection. The Quantum Cryptography will be used to encrypt the image and also used to secure the encrypted image in order to enhance the security of the encrypted image.

Any pair of parties in a network should be able to communicate, but must be authorized to do so, which requires that their identities be authenticated. The fundamental problem is how to authenticate resources to each other while minimizing the number of cryptographic keys that must be distributed and maintained, given the potential for *n*(*n* −1) / 2 pairs of communicating resources. Password or authentication key transmission may or may not be encrypted, depending on the level of risk. For quantum cryptography to succeed in practical applications, it will need to interoperate to some degree with classical networking and secure communication systems using very good network infrastructure and network firewalls. In addition, it will need to provide advantages, in cost, features, or performance that cannot be obtained with conventional methods. The most commonly cited advantage of quantum key distribution (QKD) is its ability to securely distribute one-time pads, providing truly unbreakable encryption (Scarani et al., 2009). In particular, the protocol can detect significant types of server compromise, the server cannot know Alice and Bob's shared key, and timestamps are not needed, avoiding a vulnerability of most conventional authentication protocols. The software tool used in achieving the implementation of this project work is visual C#.Net with the aid of the quantum algorithm called Peter Shor's algorithm for factoring integer numbers on a quantum computer. It is a point to note that the Shor's algorithm is designed to work on a quantum computer but this would be applied on this project work when simulating. Thus, the whole algorithm might not apply except its simulation part as regards encryption and decryption stages respectively.

The work was carried out using random secret key generation and eavesdropping detection. The Quantum Cryptography will be used to encrypt and secure the image given the potential for n(n −1) / 2 pairs of communicating resources. The design was carried out using Shor's Algorithm. This work is designed to provide an overview of the Shor's Algorithm as an encryption technique used to secure data integrity between different users of a key. Informally it solves the following problem: given an integer N, find its prime factors. Shor's Algorithm is essential because it can be used to break the widely used public-key cryptography scheme known as RSA which is based on the assumption that factoring large numbers is computationally infeasible when a quantum computer is used.

QUANTUM N SHOR'S FACTORIZING ALGORITHM

Period-Finding Subroutine: The quantum circuits used for this algorithm are designed for each choice of $\boldsymbol{N}$ and the random $\boldsymbol{a}$ used in

$$\mathrm{f(x) = ax \bmod N}, \qquad \text{find } \mathrm{Q = 2q} \text{ such that}$$
$$\mathrm{N^2 \leq Q < 2N^2} \qquad (1)$$

Which implies $\mathrm{Q/r} > N$. The input and output qubit registers need to hold superpositions of values from $0 \text{ to } \mathrm{Q} - 1$, and so have $\boldsymbol{q}$ qubits each. Using what might appear to be twice as many qubits as necessary guarantees that there are at least $\boldsymbol{N}$ different $\boldsymbol{x}$ which produce the same f(x), even as the period $\boldsymbol{r}$ approaches N/2. Proceed as follows:

i) Step1- Initialization of the registers to:

$$\mathrm{Q^{-1/2} \sum_{x=0}^{Q-1} |x\rangle|0\rangle} \qquad (2)$$

Where x runs from $0 \text{ to } \mathrm{Q} - 1$, . This initial state is a superposition of Q states.

ii) Step 2- Construction of f(x) as a quantum function and applying it to the above state to obtain,

$$\mathrm{Q^{-1/2} \sum_{x} |x\rangle|f(x)\rangle} \qquad (3)$$

this is still a superposition of Q states.

iii) Step 3- Applying the quantum Fourier Transform to the input register. This transform (operating on a superposition of power-of-two $\mathrm{Q = 2q}$ states) uses a Qth root of unity such as $\omega = e2\pi i / Q$ to distribute the amplitude of any given $|x\rangle$ state equally among all Q of the $|y\rangle$ states, and to do so in a different way for each different x:

$$U_{QFT|x\rangle=}Q^{-1/2}\sum\nolimits_{y} w^{xy}\,|y\rangle \qquad (4)$$

This leads to the final state :

$$Q^{-1}\sum\nolimits_{x}\sum\nolimits_{y} w^{xy}\,|y\rangle\;|f(x)\rangle \qquad (5)$$

This is a superposition of much more than Q states, but many fewer than Q2 states. Although there are Q2 terms in the sum, the state

$$|y\rangle|f(x_0)\rangle \qquad (6)$$

can be factored out whenever x_0 and x produce the same value.

Let ω = $e2\pi i /Q$, be a Qth root of unity, r be the period of f, x_0 be the smallest of a set of x which yield the same given $f(x)$ (where $x_0 < r$), and b run from 0 to $[(Q - x_0 - 1)/r]$

so that $x_0 + rb < Q$.

Then ωry is a unit vector in the complex plane (ω is a root of unity and r and y are integers), and the coefficient of

$$Q^{-1}|y\rangle|f(x_0) \qquad (7)$$

In the final state is:

$$\sum\nolimits_{x:f(x)=f(x_0)} w^{xy} = \sum\nolimits_{b} w^{(x_0+rb)y} = w^{x_0 y} \qquad (8)$$

Every value in the above equation represents a different path to the same result, and quantum interference occurs when the unit vectors ωryb point in nearly the same direction in the complex plane, which requires that ωry point to the positive real axis.

iv) Step 4- A measurement, some outcome y obtained in the input register and (x_0) in the output register. Since $f$is periodic, the probability of measuring some pair y and $f(x_0)$ is given by:

$$|Q^{-1}\sum\nolimits_{x:f(x)} = f()x_0\, w^{xy}|^2 = Q^{-2}|\sum\nolimits_{b} w^{(x_0+rb)y}\,|^2 \qquad (9)$$

The analysis shows that this probability is higher, the closer unit vector ωry is to the positive real axis, or the closer yr/Q is to an integer.

Turn y/Q into an irreducible fraction, and extract the denominator r', which is a candidate for r. Check if

$$f(x) = f(x + r') \leftrightarrow a^r \equiv 1 \ (\mathrm{mod}\ N) \qquad (10)$$

If so, we have a solution.

Otherwise, additional values must be obtained for r by using values near y, or multiples of r'. If any of the values hold true, it is done else, go back to step 1of the algorithm.

How Shor's Algorithm works

(1) Evaluate all values of periodic function yn mod N simultaneously.

(2) Adjust the probability amplitudes to get a value of the period r with high probability. Note: careful with a definition of which probability is considered "high." For some purposes, $1/2$ is good

enough. How? The finite Fourier transform can transform the cyclic behavior of the periodic function into the enhanced probability amplitudes of some states.

(3) Compute the procedures of Shor's Algorithm step by step above and their respective mathematical interpretation after which follow the process below for a complete Shor's workability.

The encryption process

The encryption function is encrypt(T) = (T^E) mod PQ, where T is the plaintext (a positive integer) and '^' signifies exponentiation.

Illustration:

encrypt(T) = (T^E) mod PQ= (T^17) mod 3233

To encrypt the plaintext value 123, do this:

encrypt(123) = (12317) mod 3233= 337587917446653715596592958817679803 mod 3233= 855

The decryption process

The decryption function is decrypt(C) = (C^D) mod PQ, where C is the ciphertext (a positive integer) and '^' indicates exponentiation.

Illustration:

decrypt(C) = (C^D) mod PQ= (C^2753) mod 3233

To decrypt the ciphertext value 855, do this:

decrypt(855) = (855^2753) mod 3233= 123

SYSTEM FLOWCHART

The system flow chart (Figure 1) shows the basic logic involved with authenticating a user with the quantum cryptography system. After the user enters a personal identification number, it is compared with the personal identification on file. If they are similar, access is granted to the requested file, else the user would not gain access to the system after series of trial, the system is case sensitive, thereby giving access to only authenticated users as access would be denied to eavesdroppers.

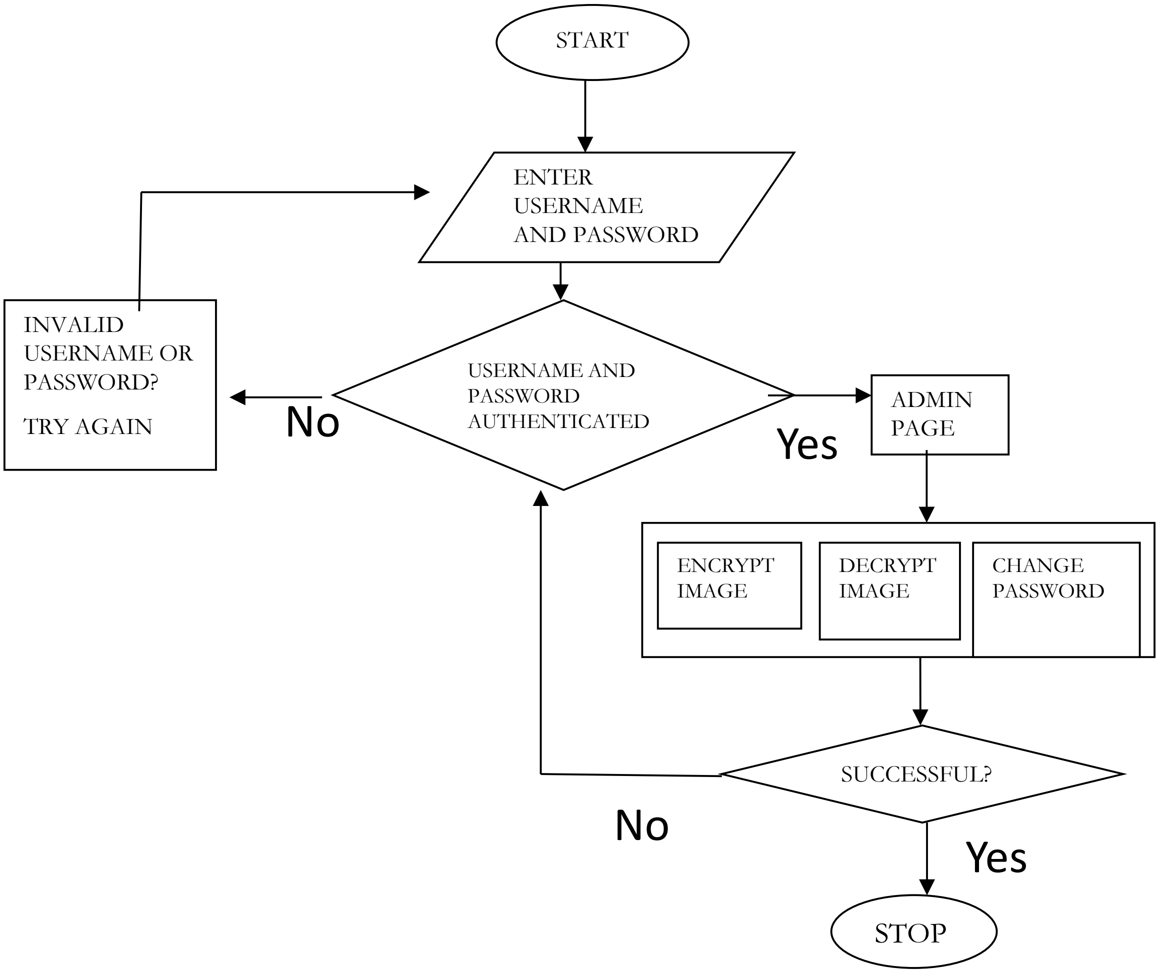

START
ENTER USERNAME AND PASSWORD
INVALID USERNAME OR PASSWORD?
TRY AGAIN
No
USERNAME AND PASSWORD AUTHENTICATED
Yes
ADMIN PAGE
ENCRYPT IMAGE
DECRYPT IMAGE
CHANGE PASSWORD
SUCCESSFUL?
No
Yes
STOP

Figure 1. Systems Flowchart

RESULT AND DISCUSSION

LOGIN PHASE OF THE SIMULATION

A predefined username and password are provided by the authorized user of the system, which would give access to the proposed system.

It is imperative to note that if neither of the username nor password is entered incorrectly, an error message prompts up denying access to the user until the correct username and password are provided.

Encryption phase of the software

Click on the encrypted image in the menu bar of the home page as shown in Figure 2.

On clicking on the encrypted image, you are launched into the encryption phase of the software where the encryption process occurs. This is shown in Figure 2.

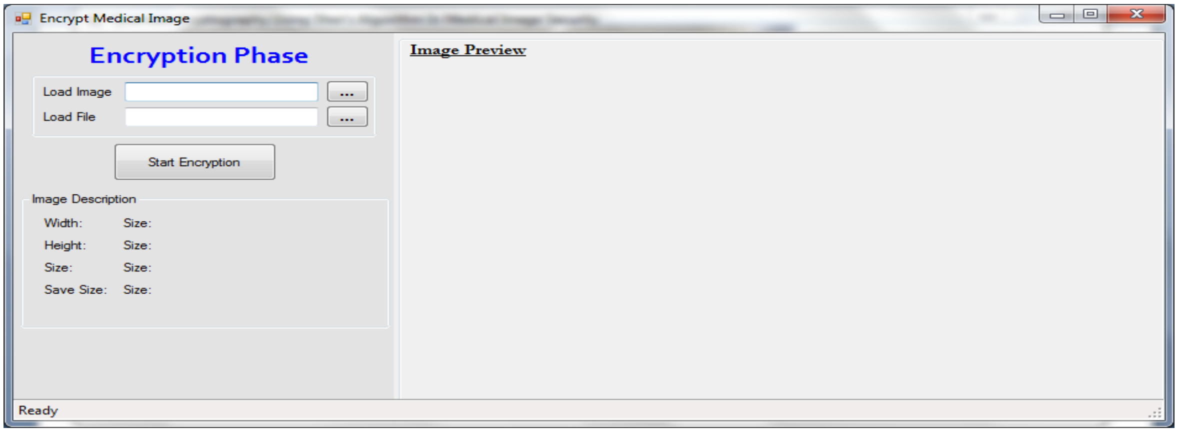


Figure 2. Encryption phase of the proposed system

Decryption phase

On clicking on the decrypted image, you are launched into the decryption phase of the software where the decryption process occurs. This is shown in Figure 3.

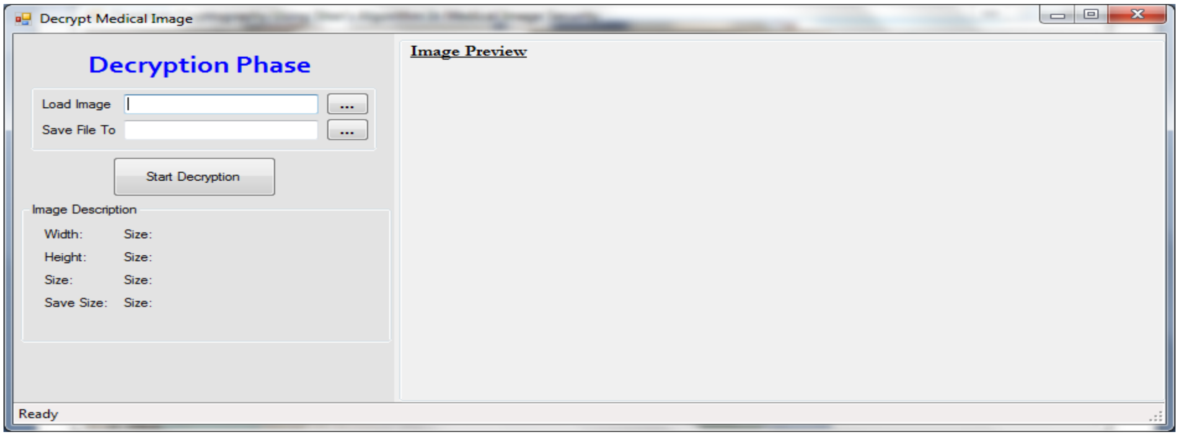
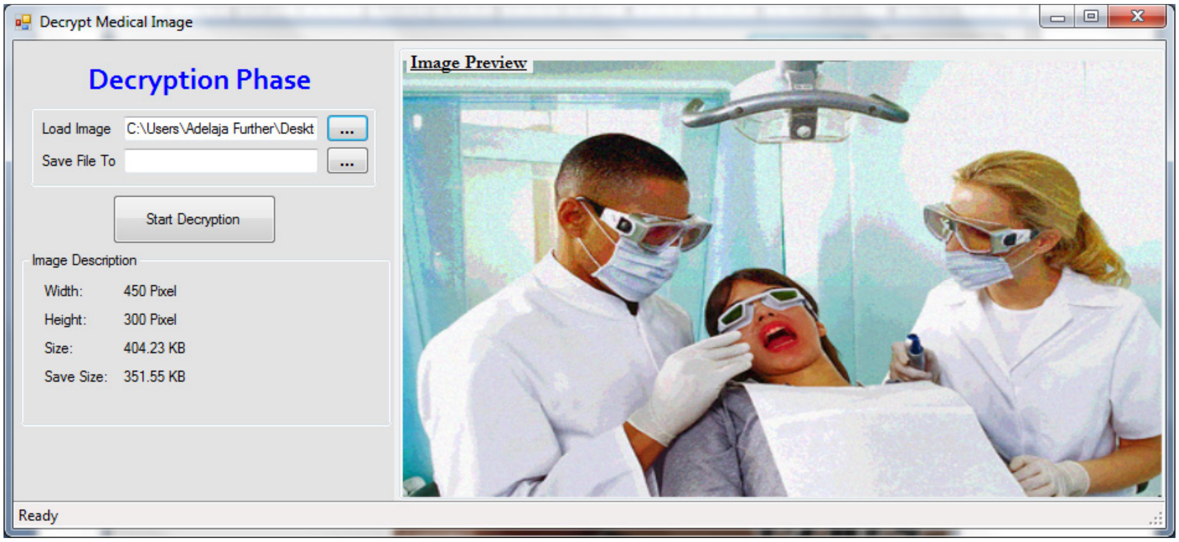


Figure 3. Loading image during decryption phase

On getting to this phase, it means you are ready to start the decryption process. First, you click on the load image; the image you are loading here is the encrypted image. You then select the image you wish to decrypt from the medical device or folder and then open it. This is shown in Figure 4.



Load Image: C:\Users\Adelaja Further\Deskt

Save File To:

Image Description

Width: 450 Pixel

Height: 300 Pixel

Size: 404.23 KB

Save Size: 351.55 KB

Figure 4. Saving file during decryption phase

After opening the file, you get this (Figure 3), and the next thing to do is to save the encrypted file to be decrypted in a folder where it would be viewed as decryption for easy accessibility. You then click save file is as shown in Figure 5.

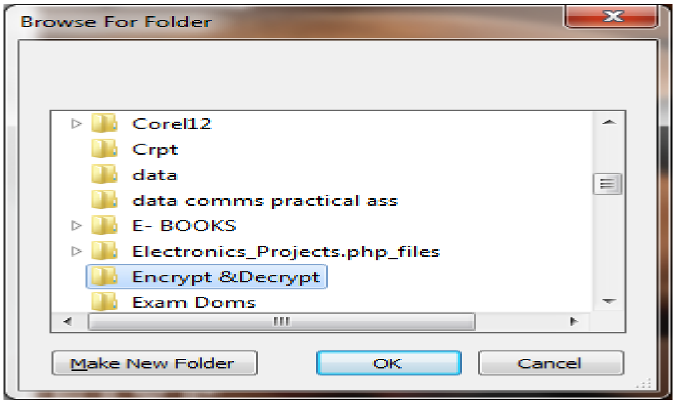


Figure 5. Folder to save decrypted files during decryption phase

Conclusion

This work has been able to point out that attaching a computer to a network increases the security risks to data that is being exchanged over the internet, the need to determine what must be protected (text and images), and how they must be protected in order to avoid eavesdropping, data hijacking, and data espionage in a medical environment. Modified Shor's Algorithm along with Data Encryption Standard (DES) that makes use of a symmetric key (secret key cryptography) in producing an encrypted version of different medial text and images were employed. The encrypted result cannot be decrypted without the encryption key, which would have been encrypted into the result of encryption processes. Also, the work has been able to point out that quantum cryptography with the application of Shor's Algorithm is a technique for limiting, if not putting an end to, eavesdroppers unauthorized access to files in a medical environment. For an effective, secured, and uncompromising security system, this work should be adopted. It is recommended that future researchers should employ the use of other encryption algorithms to develop encrypting software and overall compare all to determine the best out of all the techniques regarding speed & functionality. The implementation of this work would bring about the following: Security, Reliability, Maintainability, Portability, Extensibility, Reusability, Application Affinity/Compatibility and Resource Utilization.

In conclusion, it can be seen from the paper that quantum cryptography with the use of Shor's Algorithm is the best approach that can be employed in securing files (text and images) in a medical environment, which ends up promoting integrity of the profession and puts some assurance of no eavesdropping in the future with the patient.

REFERENCES

Abraham, N. S., & George A. (2015). A secure image transmission technique via mosaic image using HSV colour converted target image and a reversible data hiding method. *International Journal of Innovative Research in Computer and Communication Engineering, 3*(9). Retrieved from http://www.ijircce.com/upload/2015/september/123_A_Secure.pdf

Alowolodu, O. D., Alese, B., K., & Adetunmbi, O. A. (2016). Secured cloud application platform using elliptic curve cryptography. *Proceedings of the World Congress on Engineering and Computer Science (WCECS) Vol 1*. San-Francisco, USA.

Berlekamp, E. R., Mceliece, R. J., & Van Tilborg, H. C. A. (1978). On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, *24*(3), 384-386. https://doi.org/10.1109/TIT.1978.1055873

Ekert, A. (1995). What is quantum cryptography? Retrieved 12/7/02 from http://www.qubit.org/index.html

Kapur, J., & Baregar, A. J. (2013). Security using image processing. *International Journal of Managing Information Technology (IJMIT), 5*(2). https://doi.org/10.5121/ijmit.2013.5202

Lo-Varco, G., Puech, W., & Dumas, M. (2003, December). DCT-Based Watermarking Method using Error Correction Coding. In *ICAPR'03: International Conference on Advances in Pattern Recognition* (pp. 347-350).

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report, 42-44*, 114-116.

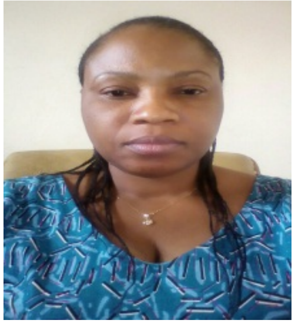
Norcen, R., Podesser, M., Pommer, A., Schmidt, H. P., & Uhl, A. (2003). Confidential storage and transmission of medical image data. *Computers in Biology and Medicine, 33*, 277–292. https://doi.org/10.1016/S0010-4825(02)00094-X

Samaan, S. S. (2016). Picture archiving and communication system design and implementation. *Al-Nahrain University, College of Engineering Journal (NUCEJ), 19*(1).

Scarani V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev. M (2009). The security of practical quantum key distribution. *Rev. Modern Physics, 81*(3). https://doi.org/10.1103/RevModPhys.81.1301

Van Der Walt, N. (2016). *The current state of quantum cryptography, QKD, and the future of information security.* MRW Labs. Retrieved from https://labs.mwrinfosecurity.com/blog/the-current-state-of-quantum-cryptography-qkd-and-the-future-of-information-security/

BIOGRAPHIES



Olufunso Dayo Alowolodu is a Lecturer I in the Department of Computer Science, Federal University of Technology, Akure. She had her Ph.D in 2016 in Computer Science. Her area of specialization includes Cyber-Security, Cloud Computing, and Cryptography.

Gabriel Kayode Adelaja is a Cyber-Security expert with the First Bank Nigeria Plc. He had his Post-Graduate Diploma in Computer Science in the year 2015. He is currently pursuing his Masters degree in the same field.

Boniface Kayode Alese is a Professor of Cyber-Security and Cryptography at the Federal University of Technology, Akure, Ondo State Nigeria.

Olufunke Catherine Olayemi is a Lecturer II in the department of Computer Science, Joseph Ayo Babalola University, Ikeji-Arakeji, Osun State, Nigeria. She is rounding-off her Ph.D and specializes in Data Mining and Machine Learning.