International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Development of a GUI for Hybrid (DES-RSA) Data Encryption and Decryption for Transmission of Biomedical Data

Adedeji Kazeem Bolade[1], Ponnle Akinlolu Adediran[2]

[1, 2]Electrical and Electronics Engineering Department, Federal University of Technology, Akure, Ondo State, Nigeria

Abstract: ***Most biomedical data are strictly confidential, hence the need to protect them from an unauthorized party. We had earlier developed and implemented a hybrid cryptography technique that uses a combination of Data Encryption Standard (DES) and Rivest Shamir Adleman (RSA) Algorithms. The DES algorithm was used to encrypt the data while the RSA algorithm was used to transfer DES secret key securely. This paper presents the development of a graphical user interface (GUI) for the developed hybrid technique. The interface was implemented in C#. The developed hybrid technique provides higher throughput, better encryption speed, and CPU power consumption usage.***

Keywords: Biomedical data, Ciphertext, Cryptography, Encryption, Graphical User Interface.

1. Introduction

Information security is an important issue in our growing information society [1]. With the increasing growth of internet and networking systems, parties tend to share or send data increasingly over communication channels. The security of such data is of paramount importance in many applications as diverse as military intelligence, medical information, government's information and service providers. The internet is a global system of interconnected computer networks that uses the standard internet Protocol Suite (TCP/IP) to serve billions of users worldwide [2]. The data is usually protected (confidentiality) before devices transmit and receive the data over transmission channels using an encryption algorithm to keep the data secure from an eavesdropper [3].

Biomedical data are majorly text and graphs/images. Biomedical data are strictly confidential and need to be secured when transmitting it over a communication channel from one physical location to the other. Indeed, the university hospital centers use and exchange several sizes and formats of medical images of patients whose contents can possess confidential information, whether it is at the level of diagnosis or at personal level, especially since these images can be remotely exchanged if the centers are interconnected by a Local Area Network (LAN) [4]. Cryptography is the science which uses mathematics to encrypt and decrypt data. This science enables one to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient [5]. The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, through a method of encryption. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key [5].

Cryptography is basically categorized into three; secret key, public key and hash function. In a secret key cryptography, a single key is used for both encryption and decryption while in the public key system uses two different (private and public) key for encryption and decryption process. The public key is used to encrypt data while the private key is used to decrypt it. Having knowledge of one key, (the public key) is insufficient in determining the private key. DES, AES, Carlisle Adams and Stafford Tavares (CAST) Algorithm, Blowfish, Twofish, IDEA and Secure and Fast Encryption Routine (SAFER) are some examples of symmetric techniques [6]. Some common examples of public key cryptographic system are RSA, Diffie-Hellman, DSA, Elgama and ECC. The RSA algorithm, at present is the most successfully use for ciphering keys and passwords or counts. [7]. All these are embedded in the elements of information security which are trust, privacy and security. The security is to maintain the confidentiality, the availability and the integrity of the information to be sent.

Few works have been done in the field of cryptography algorithms development for securing biomedical data/information. Part of this was done by Samoud and Adnen, (2012), which presents a paper on RSA Algorithm Implementation for Ciphering Medical Imaging [4]. We have carried out the development of a hybrid technique (DES-RSA) extensively and published in [8]. Therefore, this work presents the development of a user friendly graphical user interface (GUI) for the developed hybrid technique.

2. Materials and Methods

Before the description of the development of the graphical user interface, an overview of the developed hybrid technique is first presented thus:

2.1 The Hybrid Technique Implementation

The block diagram of the developed hybrid technique is shown in Figure 1. In this technique, at the transmitting side, Data Encryption Standard (DES) encryption algorithm was used to encrypt the data to be transmitted (plain text *P*) with the help of a randomly generated session key, turning it into

a cipher text. The session key was generated using pseudorandom number generator. Since DES is a secret key system, this key has to be kept secret and this is achieved by encrypting the session key using Rivest Shamir Adleman (RSA) algorithm with the help of the recipient public key. The cipher text and the encrypted session key were then sent to the receiver over a communication channel.

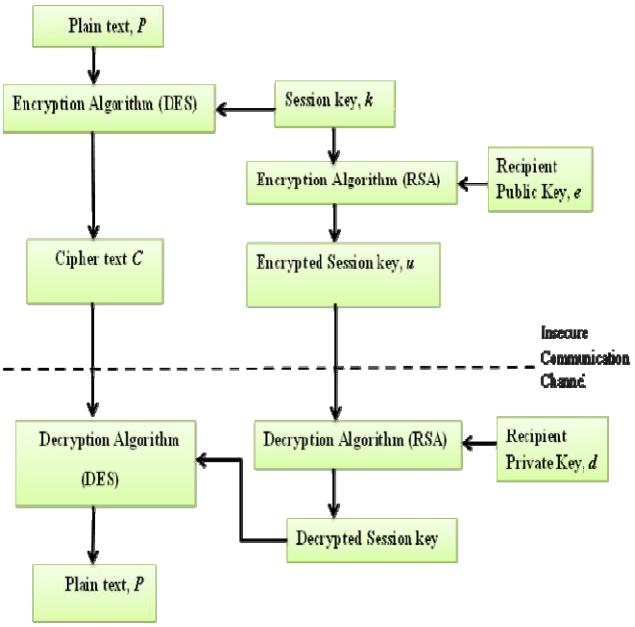

Figure 1: The developed Hybrid Technique

At the receiving end, the recipient private key was used with the RSA decryption algorithm to decrypt the encrypted session key, thereby retrieving the session key. Having retrieved the session key back; this session key was used with the DES decryption algorithm to obtain the original data (plain text *P*). The hybrid technique was implemented using C sharp language on a computer system that has the following system parameters;

1. Processor: Intel (R) Atom CPU N270 at 1.60GHz.
2. Installed Memory (RAM): 1GB
3. Operating System: Windows 7 Ultimate, 32-bit.

2.2 The Graphical User Interface Design

A graphical user interface is a type of interface that allows users to interact with the designed process environment through the use of graphical icons and visual indicators.

In visual C#, the GUI can be designed using either windows form designer (WFD) or windows presentation foundation (WPF) designer to quickly and conveniently create user interfaces. For this research, the window form designer was used because of its flexibility in handling controls. There are three basic steps in creating user interface namely;

(i) adding controls to design surface;
(ii) setting initial properties for the controls; and
(iii) writing handles for specified events.

The adding of controls entails using the mouse to drag controls, which are components with visual representation such as command button, text boxes, combo boxes etc., onto a designed surface. After controls have been added to the design surface, properties of those controls was set using the property window. Such properties includes the default text, background color, size of the form and boxes and so on. A C# source code was then written to controls or handles the events of those added buttons. This is shown in Figure 2.

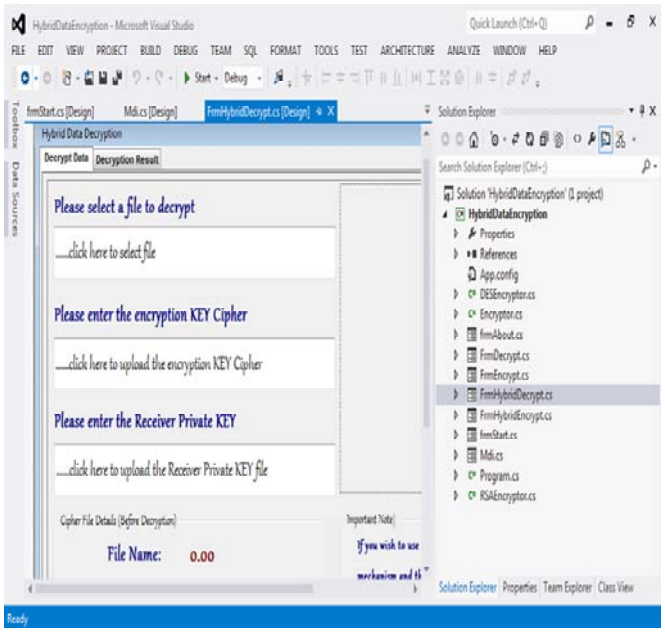

Figure 2: Window form designer in C# environment

The interface or GUI was designed to comprises of the following options; the menu selection bar where one can easily select from the drop down list either of the following data encryption scheme; DES or hybrid (DES-RSA). It also has option for user that wants to know about the project.

3. Results and Discussions

The graphical user interface for the developed hybrid technique was implemented in C#. Figure 3 shows the GUI welcome interface, which shows the title of the work and the GUI developers.

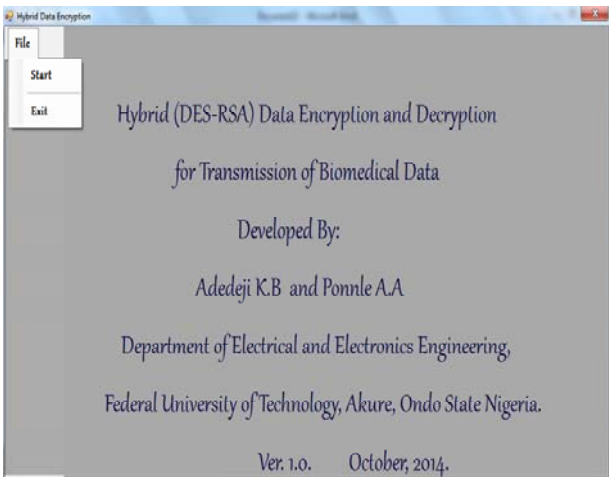

Figure 3: The GUI welcome interface

Clicking on the start menu on Figure 3, brings up the main interface as shown in Figure 4. Figure 4 shows the main interface, it includes five tabs for encryption and decryption. The user can encrypt or decrypt data according to his choice

and can also select algorithm type to encrypt and decrypt data, but for this work, hybrid technique was concentrated on.

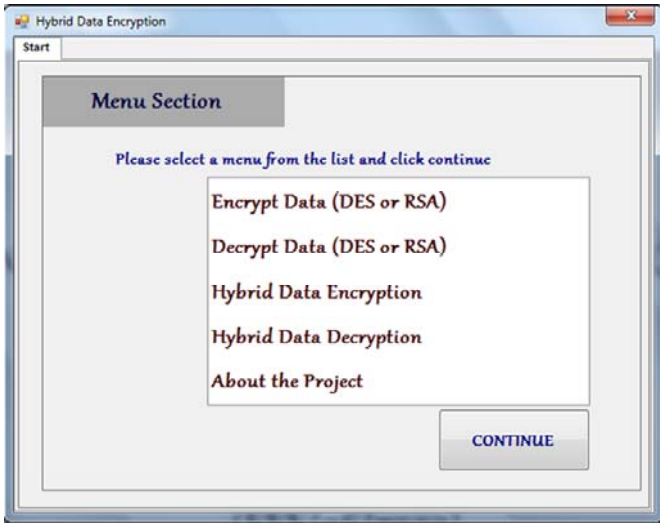

Figure 4: The GUI Main interface

Figure 5 presents how the interface can be used for encryption of data using the hybrid technique. For the hybrid technique, the user uses two keys (the public and private key). This was achieved by selecting the "generate key pair" option on the interface to generate both the public and private key pair that will be used for encryption and decryption.

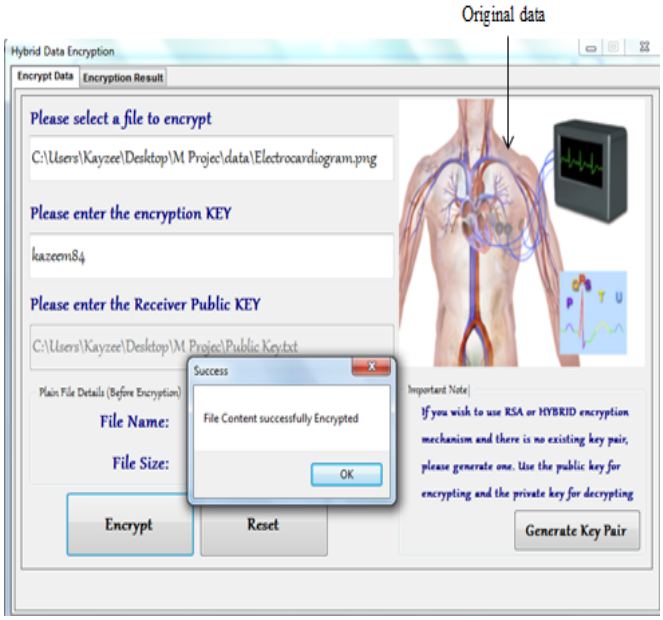

Figure 5: Hybrid files encryption

Figure 6 and figure 7 show the encrypted data and the hybrid file encryption results respectively for the image data in figure 5 that was encrypted. It can be observed from figure 6 that, the encrypted data contain only series of unreadable texts. This improves the security of the system as any adversary cannot guess correctly how the original data looks like having the information of the encrypted data only. Figure 7 is the hybrid file encryption results which include the process time of encryption and the size of the encrypted data (the ciphertext) and where the ciphertext will be saved.

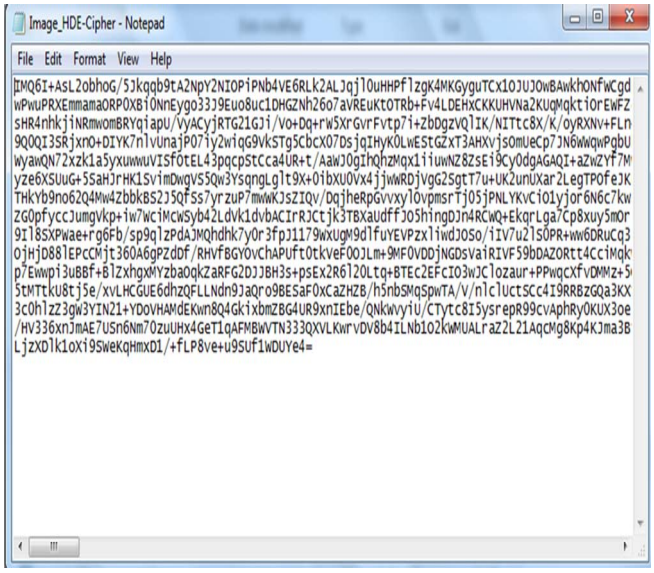

Figure 6: The encrypted data of image data in fig. 5.

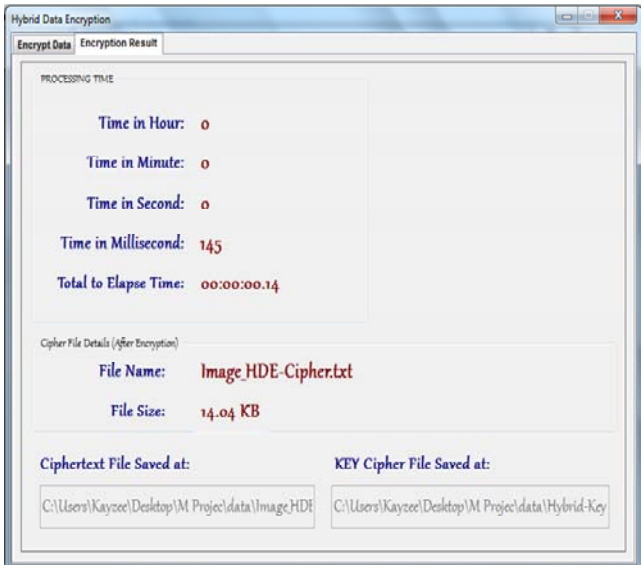

Figure 7: Hybrid file encryption result

Figure 8 and figure 9 show the hybrid data decryption and its decryption result. From figure 8 it can be seen that the original image was retrieved successfully though with a little reduction in size when compared to the original image. The reason for this is the conversion of the original image to text cipher in the encryption process. In some published works of others, the encrypted data is seen as a blurred image, which can give a little information about the input data [4], [8], [9]. The decryption result shown in figure 9 encompasses the process time of decryption, the size of the decrypted data and where it will be saved.

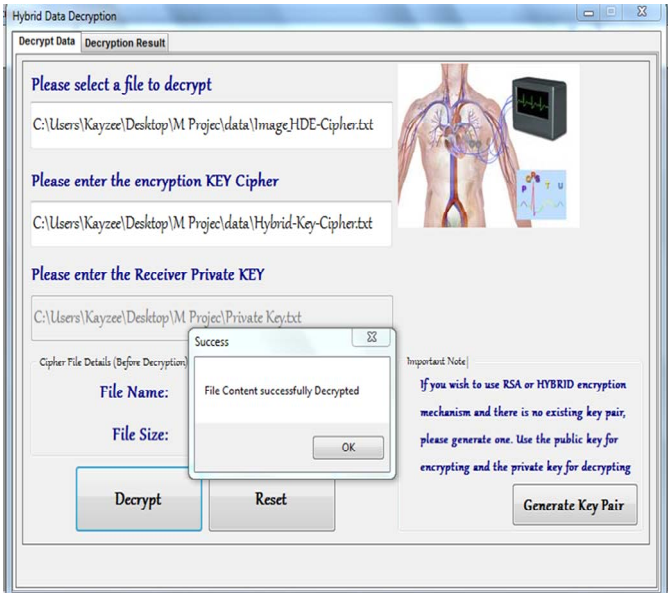

Figure 8: The hybrid data decryption

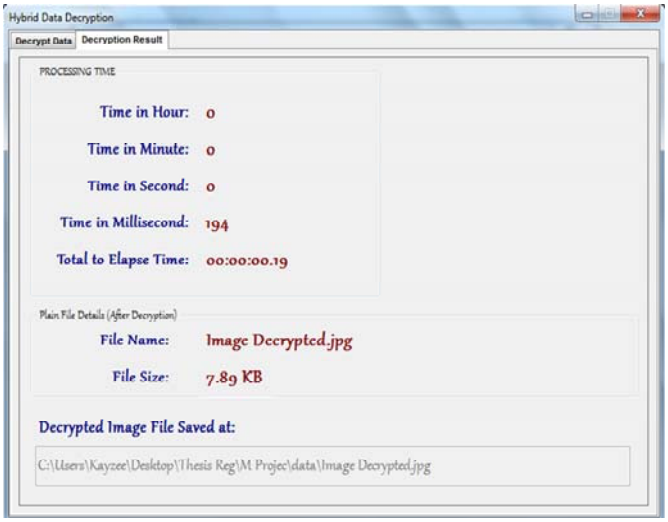

Figure 9: Hybrid data decryption result

4. Conclusion

The development and implementation of a graphical user interface (GUI) for our developed hybrid cryptography technique have been presented. This paper has shown how the developed GUI was used for encrypting and decrypting a biomedical image using the combination of DES and RSA algorithm. It can be inferred from the result presented that the developed GUI provides a friendly user environment for encrypting and decrypting biomedical signals successfully. It also provides the user the opportunity of selecting encryption algorithm of his choice to encrypt and decrypt data.

References

[1] K. Shikha, and K. Ishank, "Data Security Using RSA Algorithm In MATLAB", *International Journal of Innovative Research and Development*, Vol. 2 Issue 7, pp. 479-483, 2013.
[2] A.R. Choudhar, and A. Sekelsky, "Securing IPv6 Network Infrastructure: A New Security Model", *IEEE International Conference on Technologies for Homeland Security*, Waltham, USA, 2013.
[3] P. Prasithsangaree, and P. Krishnamurthy, "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs", Telecommunication Program University of Pittsburgh, Pittsburgh PA 15260, IEEE GLOBECOM, pp. 1445-1449, 2003.
[4] A. Samoud, and A. Cherif, "RSA Algorithm Implementation for Ciphering Medical Imaging" *International Journal of Computer and Electronics Research*, Vol. 1 Issue 2, pp. 44-49, 2012.
[5] P. Chaitanya, and Y.R. Sree, "Design of New Security using Symmetric and Asymmetric Cryptography Algorithms", *World Journal of Science and Technology*, Vol. 2, No. 10, pp. 83-88, 2012.
[6] K.M. Anand, and S. Karthikeyan, "Investigating the efficiency of Blowfish and Rejindael (AES) Algorithms", *International Journal of Computer Networks and Information Security*, Vol. 2, pp. 22-28, 2012.
[7] J.C. Borie, W. Puech, and M. Dumas, "Encrypted Medical Images for Secure Transfer". *International Conference on Diagnostic Imaging and Analysis ICDIA*, Shanghai, pp. 250-255, 2002.
[8] K.B. Adedeji, and A.A. Ponnle, "A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development", *International Journal of Scientific and Engineering Research*, Vol. 5, Issue 10, pp. 804-811, 2014.
[9] P. Singh, "Image Encryption and Decryption using Blowfish Algorithm in MATLAB", *International Journal of Scientific and Engineering Research*, Vol. 4, Issue 7, pp. 150-154, 2013.
[10] P. Kumar, and P.K. Pateriya, "RC4 Enrichment Algorithm Approach for Selective Image Encryption", *International Journal of Computer Science and Communication Networks*, Vol. 2, No. 2, pp. 181-189, 2012.

Author Profile

Adedeji Kazeem Bolade received B.Eng. degree in Electrical and Electronics Engineering from Federal University of Technology, Akure, Nigeria in 2010 and he is currently pursuing M.Eng. degree in the same Institution. His research interest includes network security and data communication systems. He is presently a Research Assistant in the department of Electrical and Electronics Engineering, Federal University of Technology, Akure, Nigeria.

Ponnle A. A. obtained B. Eng. and M. Eng. degrees in Electrical and Electronics Engineering from Federal University of Technology, Akure, Nigeria in 1998 and 2003 respectively, and obtained PhD degree in 2011 from Tohoku University, Japan. His research interest includes digital signal processing, electronics, communication systems and biomedical engineering. He currently teaches in the department of Electrical and Electronics Engineering at both undergraduate and postgraduate levels in Federal University of Technology, Akure, Nigeria. He is a member of Nigeria Society of Engineers (NSE).