Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 4, No. 4, December 2016, pp. 307~318
ISSN: 2089-3272, DOI: 10.11591/ijeei.v4i4.241

Improved Image Encryption for Application over Wireless Communication Networks using Hybrid Cryptography Technique

Adedeji Kazeem B*, Ponnle Akinlolu A
Department of Electrical and Electronics Engineering, Federal University of Technology, Akure,
Ondo State, Nigeria.
e-mail: kezman0474@yahoo.com*, akinloluponnle@yahoo.co.uk

Abstract

Advances in communication networks have enabled organization to send confidential data such as digital images over wireless networks. However, the broadcast nature of wireless communication channel has made it vulnerable to attack from eavesdroppers. We have developed a hybrid cryptography technique, and we present its application to digital images as a means of improving the security of digital image for transmission over wireless communication networks. The hybrid technique uses a combination of a symmetric (Data Encryption Standard) and asymmetric (Rivest Shamir Adleman) cryptographic algorithms to secure data to be transmitted between different nodes of a wireless network. Three different image samples of type jpeg, png and jpg were tested using this technique. The results obtained showed that the hybrid system encrypt the images with minimal simulation time, and high throughput. More importantly, there is no relation or information between the original images and their encrypted form, according to Shannon's definition of perfect security, thereby making the system much more secure.

Keywords*: cryptography, digital image, eavesdropper, security, wireless networks*

1. Introduction

A large amount of digital data is being sent over wireless communication channels due to rapid growth of technology in data communication. A wireless network is a collection of nodes organized into a cooperative network. The transfer of digital information over a wireless network has opened opportunities for collecting/sharing large data [1]. These transmitted digital information are confidential or private and therefore demands for security mechanisms to provide required protection. Security has been a major challenge for data transmission over wireless networks for the past few years. This is due to the open nature of wireless channel, making it possible for adversaries or eavesdropper who is assumed to have adequate computing power and resources to decode any message transmitted over a wireless network. For secured communications between the two nodes, three main security goals must be achieved [2]. These are confidentiality/secrecy, data integrity and service availability. Confidentiality ensures that the data to be transmitted is prevented from unauthorized users. It means that only the authenticated recipients are able to interpret the message (data) content and no one else. Data integrity prevent it from undergoing any form of alteration during transmission between the two ends of the nodes (sender and receiver), while service availability ensures that it is available to its intended users [3, 4].

Digital images in many applications are confidential data and their encryption is being applied in internet communication, multimedia systems, tele-medicine and military communication to mention a few [5-7]. Most government parastatals, military intelligence, forensic departments, financial institutions, hospitals and private business all deal with confidential messages. For example, hospitals deal with information about their patients, geographical areas in forensic departments, enemy positions in military intelligence, and product financial status in case of financial institutions. During their transmission especially over the internet, the content can be accessed illegally and misused by unauthorized parties [8]. These information needs to be protected from an unauthorized person when being transferred over wireless communication networks.

There are three different ways to protect digital image from unauthorized use or access. These are cryptography, steganography and watermarking [9]. Steganography serves to hide

Received August 24, 2016; Revised October 16, 2016; Accepted November 20, 2016

secret messages in other messages or graphics. Generally the sender embeds the secret message in an innocuous written message on the same piece of paper [10, 11]. More recently, steganography involves hiding secret messages in graphic images by replacing the least significant bit of each byte of the image with the bits of the message. Watermarking is related to steganography in the sense that it tries to hide a message related to the actual content of the digital signal, but in steganography, the digital signal has no relation to the message and merely used as a cover to hide its existence [12].

Cryptography schemes are widely used among these techniques and have been applied for protection of digital data in the past few years. Cryptography is an algorithmic process of converting a plain data to a cipher text, a form that is unreadable by an unauthorized person (eavesdropper) [13-14]. This technique is usually achieved with the use of an encryption key to alter the message based on the key bits resulting in a cipher text (encrypted data) as given in equation (1)

$$C = E\left(K,P\right) \tag{1}$$

In equation (1), C is the encrypted data (cipher text), E(.) is the encryption function, K is the encryption key and P is the original data to encrypt. The encryption algorithm operates on the plain data with the use of an encryption key to obtain the cipher text. The decryption process is the reverse of the encryption. According to Shannon’s definition for perfect security, the result of encryption of the message (cipher text) must not provide any information on the original text (plain text) [15, 16]. Cryptography algorithms are of three types namely; symmetric key cryptography (SKC) or private key cryptography, asymmetric key cryptography (AKC) or public key cryptography, and hash functions [8, 17]. Symmetric key cryptography technique which provides a faster means of encrypting and decrypting data, uses a single key for both encryption and decryption process [8, 18]. The problem with this type of system is the key management. Since it uses one key for both encryption and decryption, if the key get exposed or known by an eavesdropper, the whole system collapse and the eavesdropper will be able to decode any message sent from the source node to the receiver’s node. Some examples of this type of system are Data Encryption Standard (DES), Rivest Cipher4 (RC4), Advanced Encryption Standard (AES), Blowfish Algorithm, Twofish Algorithm, International Data Encryption Algorithm (IDEA) and Secure and Fast Encryption Routine (SAFER) [19, 20].

The problem of key management in symmetric key cryptography technique was overcome in asymmetric key cryptography technique by employing two keys for encryption and decryption process. In this system, one key called the secret key is used for encryption while the other key called the public key is used for decryption [21]. By using one key for encryption and another key for decryption, the problem of key management was overcome. Having the knowledge of one key is not sufficient to decode the message [21]. However, this type of system is very slow and computational more demanding than the SKC [22]. Some examples of this type of systems includes; Rivest Shamir Adleman (RSA) algorithm, Elgama, Deffie-Hellman, Digital Signature Algorithm [23]. The harsh function such as message digest (MD), secure harsh functions (SHA-1 and SHA-2) uses a mathematical transformation to encrypt information [24].

More recently, image encryption has been studied in [8, 25-29] to meet the demand for real-time applications over wireless communication networks. More also, it was reported in [8] that protecting images is an ethical and legal requirement. Different work in [9, 14, 28-30] have been conducted to secure and improve security of digital images over a wireless communication channel. Some authors [6, 29, 30] achieved encryption using a chaotic system, while others [31] use the same symmetric and asymmetric algorithms or a combination of both to improve security in wireless communication network.

With advancement in technology, wireless communication channel will become more flexible in terms of sending large amount of confidential data across it. This advancement in technology also translates to development of sophisticated deciphering algorithm by eavesdroppers prompting for the need to improve security of data before sending over a wireless sensor network. The objective of this work is to improve the security of digital image transmission by employing a hybrid cryptographic technique that we developed. This technique combines the speed of the symmetric cryptography technique and the key management of the asymmetric cryptography technique.

2. Research Method

The developed hybrid technique uses a combination of data encryption standard (DES) and Rivest Shamir Adleman (RSA) algorithms.

2.1. DES Encryption and Decryption Process

The DES uses a 56 bit key (an equivalent of 8 byte) to encrypt the digital image. There are three main stages involved in the process of encrypting and decrypting the digital image using this technique [31, 32]. These stages include; an initial permutation on the word length of the image pixel, a 16 rounds of complex key dependent computations where each of the word length is divided into two halves (left L and right R) from the initial permutation of the image and is combined with the key bits. The sixteen round of key dependent operation is given the relation shown in equation (2)

$$\left.\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f\left(R_{i-1}, K_i\right) \end{aligned}\right\} \text{for } 1 \le i \le 16 \tag{2}$$

In equation (2), K is the DES key and i depicts the number of rounds (16 rounds in this case). After the sixteen rounds, the left and right halves were combined after which a final permutation is applied to obtain the encrypted digital image. For decryption, the encryption process is reversed to retrieve the original image.

2.2. RSA Encryption and Decryption Process

RSA encryption scheme uses prime numbers and base its security in the difficulty involved in factorizing the product of two large numbers. Since this is an asymmetric key system, it requires two different keys for encryption and decryption process which must be generated first. For RSA key generation algorithm, random numbers were first generated using pseudo-random number generator (PNG) from which two distinct large numbers p and q were selected by the algorithm. Primality test was then performed on the chosen numbers to check whether the numbers are prime. If p and q passes the primality test, then the algorithm proceed to compute the product of p and q as n and the Euler's totient function. The Euler's totient function given by

$$\varphi(n) = (p-1)(q-1) \tag{3}$$

In case *p* and *q* or anyone of them is not a prime number (fails the primality test), it returns to select another *p* and *q*. Also, an integer *e,* which is the RSA encryption (public) key was chosen. The encryption key selection is based on equation (4) given as

$$\left.\begin{aligned} &1 < e < \varphi(n) \\ &\gcd\left(e, \varphi(n)\right) = 1 \end{aligned}\right\} \tag{4}$$

In equation (4), *e* is relatively prime to ***ϕ(n)***. The interpretation of this is that the greatest common divisor (gcd) between the RSA encryption key and the Euler's totient function must not be any other number other than one. To improve security and effectiveness of the system, *p* and *q* must be of the same lengthin bits, must not be equal and they should not be too close to each [33]. The next stage after the encryption key selection is the computation of the RSA private key *d,* computed using the Extended Euclidean Algorithm given in equation (5)

$$d \times e = 1 \bmod \left(\varphi(n)\right) \tag{5}$$

From equation (5), the RSA private key is given as

$$d = e^{-1} \bmod \left(\varphi(n)\right) \tag{6}$$

a. The Hybrid Image Encryption and Decryption Technique

In the developed hybrid technique which uses a combination of DES and RSA, DES was used to encrypt the digital image due to its fast response (simulation time) while RSA was used to encrypt DES session key (secret key). The flow chart of the entire digital image encryption using this technique is shown in Figure 1.

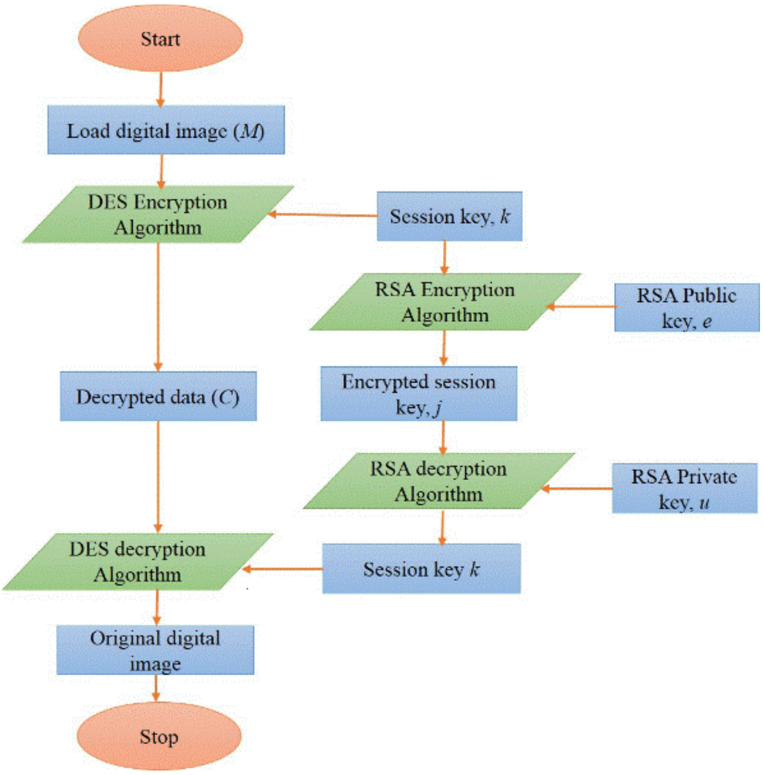


Figure 1. Flow chart of image encryption and decryption using the developed hybrid technique [32].

From the figure, the digital image M, loaded into the system was made to pass through a DES encryption algorithm using DES session key k. The output of this process results in an encrypted data C. More also, the DES session key was passed through a RSA encryption algorithm using RSA public key e, thereby resulting in an encrypted session key j. These two encrypted data (C and j) was then sent to a receiver over a communication channel. Since DES is a symmetric key cryptography system (uses the same key for encryption and decryption), a recipient at the receiving end, uses his RSA private key d, to retrieve the DES session key before using this on DES decryption algorithm to obtain the original image. The four main processes involved in the hybrid system and the operation in each of the stages are given below:

(i) DES encryption of the digital image: the output of this stage is the encrypted data given in equation (7)

$$C = E(k, M) \tag{7}$$

(ii) RSA encryption of DES session key: this results in an encrypted session key given by

$$j = k^{e}\left(\mathrm{mod}\left(n\right)\right) \tag{8}$$

(iii) RSA decryption of DES session key: this results in a decrypted session key at the receiving end given by

$$k = j^{d}\left(\mathrm{mod}\left(n\right)\right) \tag{9}$$

(iv) DES decryption of the encrypted image: results in the original digital image given in equation (10)

$$M = D\left(C,k\right) \tag{10}$$

The hybrid cryptographic technique was implemented using Microsoft visual C# platform on Intel (R) Atom (TM) CPU N270 with 1.6GHz processor speed, 2GB RAM, running windows 7 operating system. The image encryption and decryption was done by loading three image samples (of different formats) into a graphical user interface (GUI) developed in [34] to facilitate easy use. Properties of the three image samples are shown in Table 1.

Table 1. Properties of the selected digital image

S/N	Image Type	Dimension	Image Size (kB)
1	jpeg	290x174	14.37
2	png	500x304	118.91
3	jpg	300x168	6.67

For performance analysis, the speed and CPU power usage during encryption and decryption process was determined. Also, the encryption and decryption time were recorded for each image encryption/decryption process from the developed GUI. More also, the throughput during each process was also calculated which gives an indication of the CPU power usage during these two processes. The throughput TR, and the encryption ratio ER, are given by equation (11) and equation (12) [35].

$$TR = \frac{\sum M_t}{\sum E_t} \tag{11}$$

$$ER = \sum\left(\frac{L_y}{L_x}\right) \tag{12}$$

where M_t is the size of the image to be encrypted/decrypted and E_t is its corresponding encryption/decryption time. In equation (12), L_y is the size of the encrypted data while L_x is the size of the original data.

3. Results and Discussions

3.1. Image Encryption and Decryption

Figure 2(a) shows a digital jpeg type image and Figure 2(b) shows its encrypted data using the developed hybrid technique. Considering the figure, it can be observed that the encrypted data provides no information about the original image. Thus meeting Shannon's definition of perfect secrecy [15]. Figure 3 and Figure 4 show the encryption for png and jpg type images.

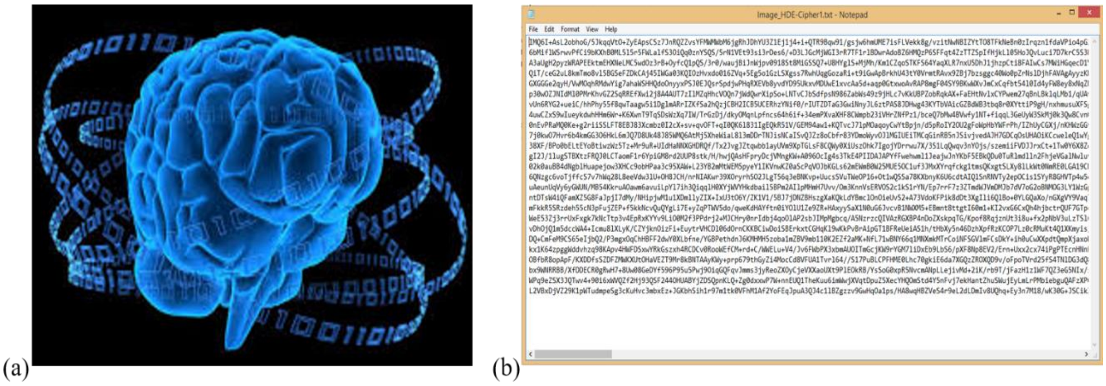


Figure 2. Image encryption for a jpeg type image (a) original image and (b) encrypted data using the hybrid technique.

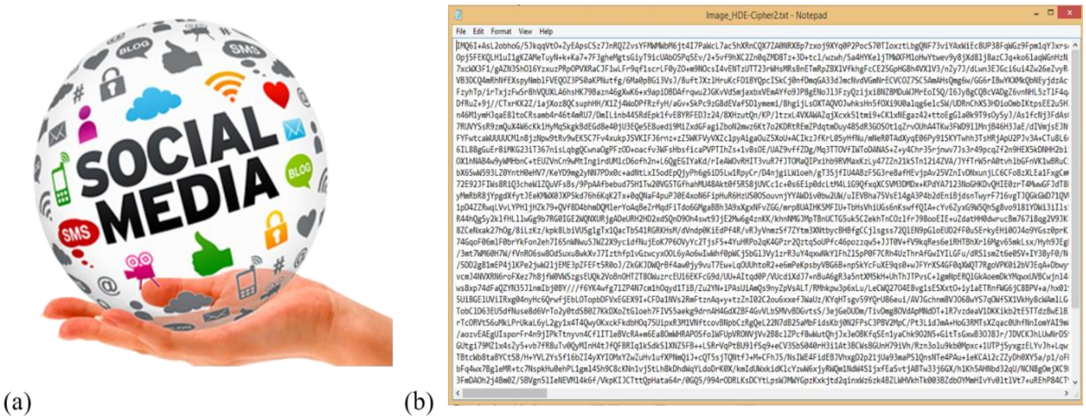
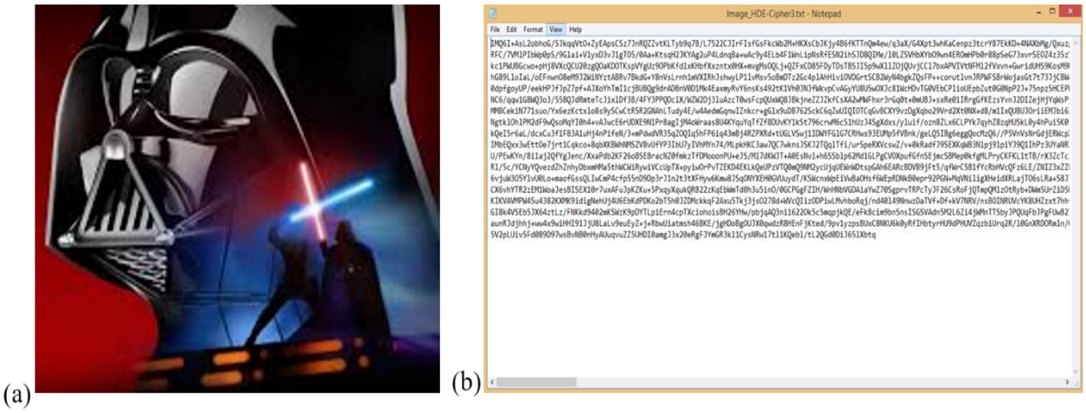


Figure 3. Image encryption for a png type image (a) original image (b) encrypted data using the hybrid technique.



```
IMQ6I+AsL2obhoG/5JkqqVtO+ZyEApsCSz7JnRQZZvtKLTyb9q7B/L7522CJIrFIsfGsFkcWb2M+HKXsCbJKjy4B6fKTTnQm4ew/q3aX/G4Xpt3whKaCenpz3tcrY87EkKD+4NAXbMg/Qxuz
RFC/7VM1PIbWp0pS/9Glai+VlyxD3vJ1gT05/0Aa+KtsqH2JKYAg2uP4LdnqBa+wAc9y4ELb4F1WnLipNsRfESN2ihSJD8QIMe/10LZSVHbXYbO9wn4EROmHPb0r88pSeG73xvrSEOZ4z35z
kc1PWUBGcwo+pHj8VXcQCU20zgQOaKDOTKspVYgUz9OPbKfd1xKHbfXxzntx0HX+mvgMsOQLj+QZFxCD85FDyTDsTBSJI5p9wX11ZOjQUvjCC17bxAPVIVtNFM12fVxvn+GwridUHS9KosM9
hG89LloIaL/oEFnwn08eM9J2WiNYztABRv7BkdG+Y8nVsLrnh1mVXIRhJshwyLP1lvMsv5o8mDTz2Gc4plAhHiv1OVDGrtSCB2WyN4bgkZQsFP++corutlvnJRPWFSBrWojasGt7t73JjCBW
0dpfgoyUP/eekHPJfJpZ7pf+AJXoYhTmI1cjBUBQg9drAD8nV0D1Mk4EaxmyRvY6nsKs492tK1Vh0JNJfWkvpCvAGyYU8U5wOXJc81WcHDvTG0VEbCP1ioUEpbZut0G0NpP2J+75npz5HCEP
NC6/qqw1G8WQ3o3/558QJdRmteTcJix1Df3B/4FY3PPQDc1X/WZW2Dj3luAzcT0wsFcpQUxWQ8JBkjneZZJZkfCsXA2wMWFhxr3rGq0t+0mUBJ+sxRe01IRrgGfKEzsYvnJ2DIZejHjYqWsP
MMBCekiN771suo/Yx6ezKctxlo8s9ySCwCtR5R2GNAhLTudy4E/w4AedmGqnwIZnkcr+gGlx9uDB762SckC6qZwUIQIOTCqGvBCXY9vzDgXqbo29Vrd2Xt0NX+d8/m1IxQU8UJOriiEMJbi6
Ngtkl0h1PM2dF9wQsoMqYI0h4+vAJwcE6rUDXE9N1Pr8agIjM4oWraas8U4KYquYqTfZf8DUvKY1kSt796crwM6cS1hUzJ4SgXdxs/yluif/ozn8ZLx6CLPYk7qyhZ8zqHUSkL0y4hPu15K0
kQeI5r6aL/dcxCu3f1F83A1uHj4nPifeN/3+mPdwdVR35qZOQIq5hFP6iq43mBj4RZPXRd+tUGLVSwj1IDWYFG1G7CRHws93EUMp5fVBnk/geLQ5IBg6eggQocMzQ6//P5VnVsNrGdjERWcp
IMbEQxx3wEttOe7jrt1Cqkco+8qbXKBWhNMSZV8vUfYP3IbU7yIVhMYn74/MLpkHKC3aw7QC7wknsJSKJ2TQq1Tfi/urSpeRXVcswZ/v+0kRadfJ9SEXKqWB3N1pj91piYJ9Q1IhPz3UYaNR
U/PEwKYn/81iaj2QfYgJenc/XxaPdb2KF26o8SE8racNZ0fmkzTfDMooonPU+eJS/M17dKWJT+A0EsNv1+h6SSb1p62Md1GLPgCVOXpufGfnSEjmcS8Mep0kfgMLPryCKFKL1tTB/rX3ZcTc
R1/5c/YCNyYQvezdZhZnhyObxmHMa5thWCWiRywiVCcUpTX+pyiwOrPvTZEKD4EKLkQeUPzVTQ0mQ9NM2ycUjqUEWnWDtspGAh6EARcBDVB9jFt5/qfWrC5B1fYcRbHVcQFz6LE/ZNIZ3xZZ
6vjuW305Y1vU0Lo+maofGssQLIwCmP4cfp55nD9Op3rJ1n2t3tXFHyw6Kmw8JSqONYXEH0GVUuydT/KSWcnxWpEiVwBaOHsf6WEpRDNkB0epr92PGN+MqVNi1igXHeidXRLajTO6sLRa+S8J
CX6vhYTR2zEM1WoaJesBISEX10r7uxAFuJpKZKu+5PxqyXqukQRB22zKqEbWmTd0h3u5inO/0GCPGgFZIH/WnHNbVGDAiaYwZ70SgprvTRPcTyJF26CsRoFjQTmpQM1zOtRyb+DWm5UrZ1DS
KIKVAVMPW45u4382KXMK9idigNehUj4U6EbKdPDKo2bT5h0JZDMckkqF2Axu5Tkj3js0278d+WVcQIizODPiwLMvhboRqj/nd40149NnwzDaTVf+Df+kV7NRV/nsBOINRUVcYK8UHZzxt7hh
GI8k4VSEb5JX64ztLz/FNKkd9402mKSWzK9pDYTLpiErn4cpTXciohoisBH26YHw/pbjqAQ3ni16220k5c5mqpjkQE/eFk8cim9bnSnsISGSVAdn5M2L6Zi4jWMnTTSbyJPQUqFbJPgFUwB2
aunRJdjhhj+ww4x9wiHHI91JjU8LaLv9euEyZ+j+RbwUiatmsh46BKE/jgHDoBgOUJX0qwdzRBHEnFjKted/9pv1yzpsBUxC8NKU6k0yRfIHbtyrHU9dPHUVZqzbiUrq2R/10GnXRDORmln/
5V2pLUiv5Fd089O97wsBvNB0nHyAUuqvuZZ5UHDI0amgJ3x20eRgFJYmGR3k11CysNRw17t11KQeb1/tL2QGd0DiJ651Xbtq
```

Figure 4. Image encryption for a jpg type image (a) original image (b) encrypted data using the hybrid technique.

Also in line with Figure 2, the original images and their encrypted form are statistically independent. The mutual information between them is zero. It can be observed from the presented figures that a perfect security was achieved which improves the security of the digital image. In the research works of the authors in [27, 36], there is still little information between the original image and its encrypted form. However, the hybrid technique used for this image encryption has achieved security as illustrated in the results of the encryption presented above.

Figure 5, Figure 6 and Figure 7 show the histogram of the original and the encrypted image for the three tested image data type. In these figures, it is observed that the statistical pattern of both the original image and its encrypted form is totally different for each of the image type. The correlation between the two data can be said to be zero as there is no statistical correlation between them; thus meeting Shannon’s definition of perfect secrecy, thereby enhancing security.

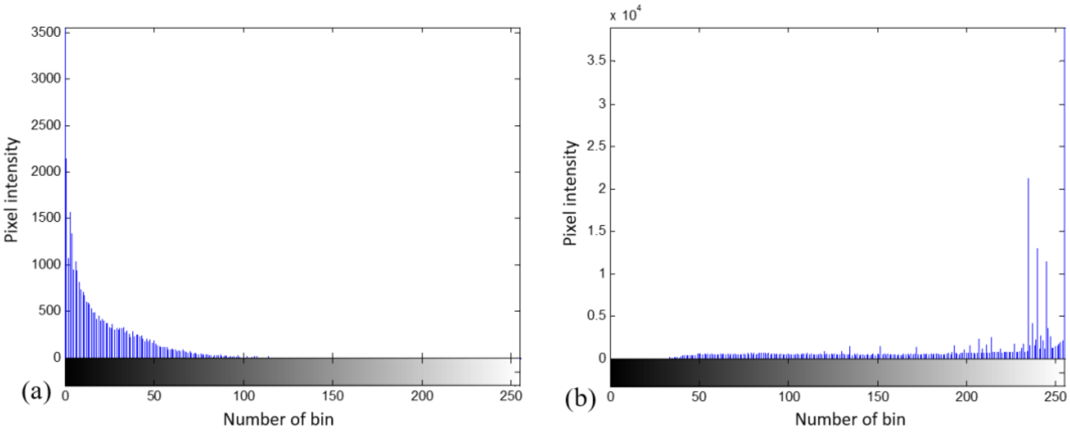


Figure 5. Histogram plot for the jpeg type image (a) original image (b) encrypted data.

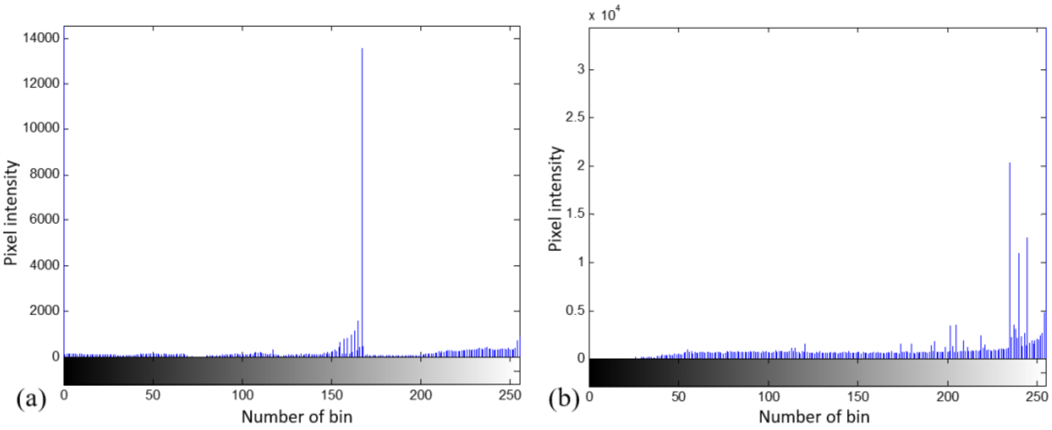


Figure 6. Histogram plot for the png type image (a) original image (b) encrypted data.

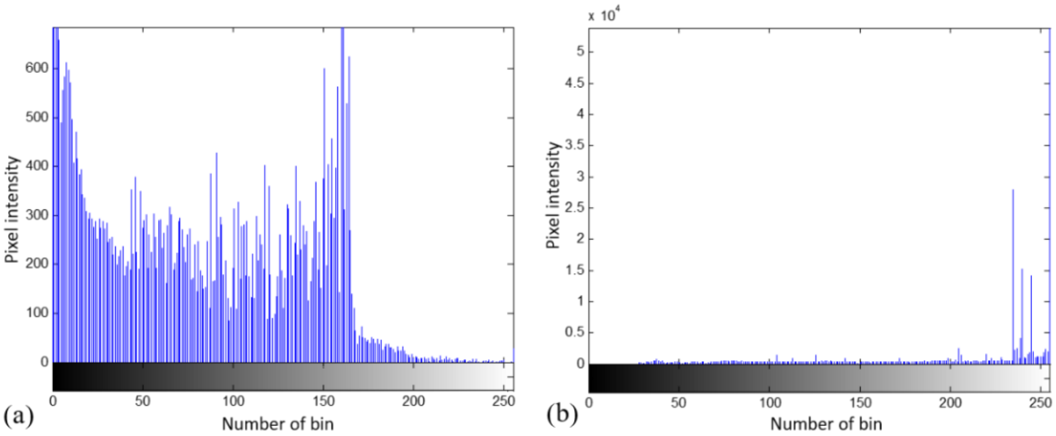


Figure 7. Histogram plot for the jpg type image (a) original image (b) encrypted data.

Moreover, to further analysis the degree of correlation between the original and the encrypted image, we present in Figure 8 to Figure 10, the scatter plot of these data. Looking at these figures, the RGB pixel pattern for the original image of each image type is different when compared to their corresponding encrypted form. While the pixel pattern of the encrypted images clusttered together at most point on the plot, a different orientation is observed for the original data.

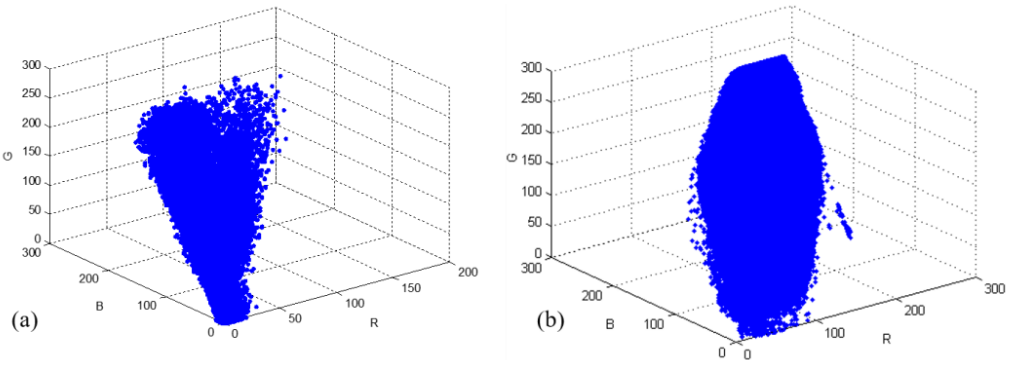


Figure 8. Scatter plot for the jpeg type image (a) original image (b) encrypted data.

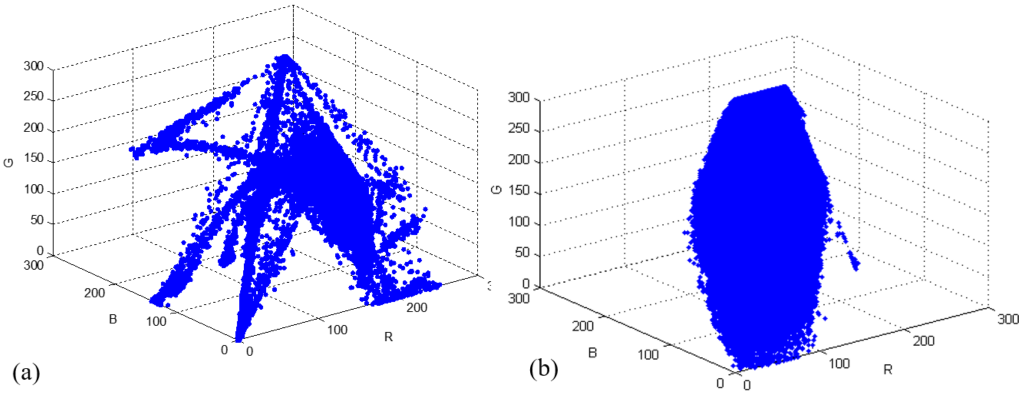


Figure 9. Scatter plot for the png type image (a) original image (b) encrypted data.

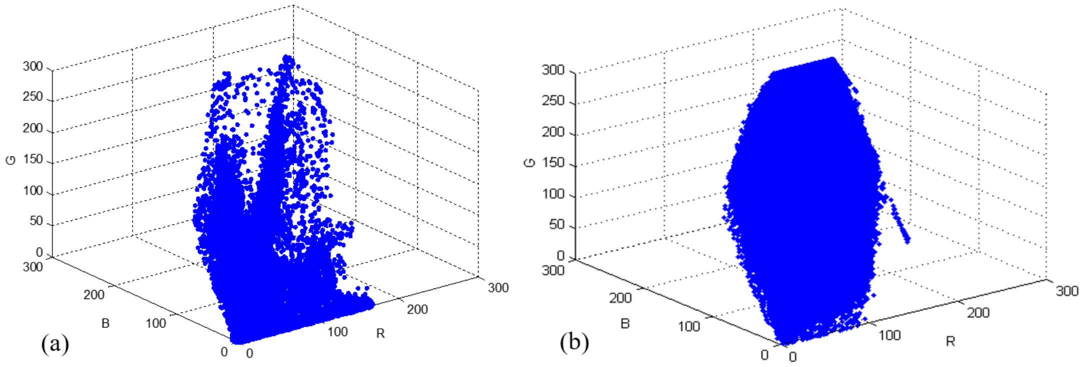


Figure 10. Scatter plot for the jpg type image (a) original image (b) encrypted data.

3.2. Simulation Time and Throughput

The simulation time, throughput and the encryption ratio achieved using this technique is shown in Figures 11-13. Considering Figure 11, one can see that the simulation time is higher during encryption process for jpeg and png type images. However, for jpg type image the decryption time is higher than its encryption time. The simulation time for each of the three images is less than one second, depicting high speed of encryption and decryption achieved by the technique.

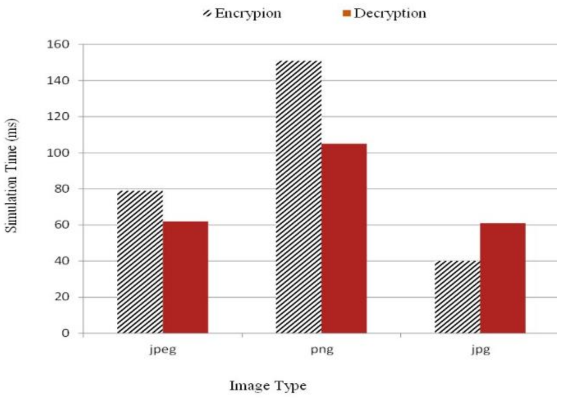


Figure 11. Encryption and decryption time for the tested images.

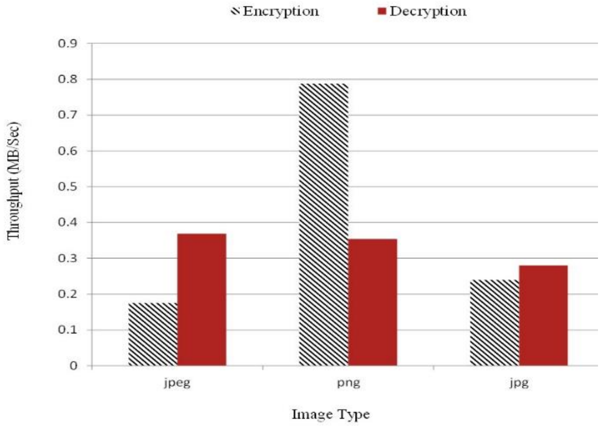


Figure 12. Throughput of encryption and decryption for the tested images.

The throughput for both the encryption and decryption process is shown in Figure 12. Considering the figure, both the png and jpg type image has a higher throughput for their encryption process with respect to their decryption process. However, in jpeg type image, the throughput for decryption process is a little bit higher than the encryption process. In general, higher throughput translates to lower CPU power consumption usage by the algorithm [35]. It can be observed that, the png type image which has larger size than the jpeg and jpg type image has the highest throughput, which means it consume less power during encryption.

Figure 13 shows the encryption ratio for the selected images. For text data, the size of the decrypted text must be equal to the original text size [9] making the encryption ratio to be one. However, this is not a requirement for image data, a small distortion in the decrypted image is acceptable [9]. Considering the figure, the encryption ratio in each case is not equal to one which is in line with Narendra [9]. It can also be observed that the encryption ratio of the png type image is lower than that of jpg and jpeg type images. This means that the size of the encrypted data for the png is small compare to the original image. This consumes lesser bandwidth for transmission and storage over wireless networks. Therefore, transmitting large sizes of digital images over wireless communication networks using this technique is possible as it provides a better bandwidth utilization.

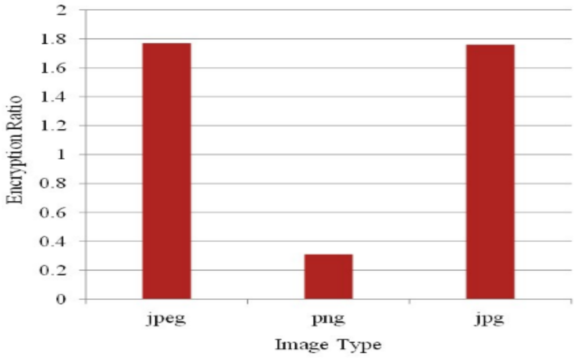


Figure 13. Encryption ratio for the tested images.

4. Conclusion

Digital image encryption has been achieved using hybrid (DES-RSA) cryptographic technique for applications over wireless communication networks. The overall simulation results yield useful information. The technique gives an improved security of the selected images according to Shannon's definition of perfect security. Also, the technique gives a low simulation time for the encryption and decryption process and lower throughput for the tested image samples. Hence, the hybrid technique for image encryption and decryption will adapt well in applications where security demand is a requirement, with fast simulation time. This technique will contribute to improving security of digital image for applications over wireless communication and sensor networks. More also, the results obtained showed that the hybrid technique will be more useful for real-time applications involving sending larger sizes of digital images over wireless communication networks without consuming much bandwidth and power.

References

[1] Varshini R.S, Vijendra D.B. *Encryption and Fusion of Target Decision based on Channel Gain in Wireless Sensor Networks.* In: International Conference on Signal Processing, Embedded System and Communication Technologies and their Applications for Sustainable and Renewable Energy. 2014:198-206.

[2] Earle G. Wireless Security Handbook. Auerbach Publications. Florida, United States. 2005.

[3] Ahmed M, Sanjabi B, Aldiaz D, Rezaei A. Omotunde H. Deffie-Hellman and its Application in Security Protocols. *International Journal of Engineering Science and Innovative Technology*. 2012; 1(2): 69-73.

[4] Nurul A.R, Zafran A, Habibah H, Farid A, Anuar I. *Cryptographic Computation using Elgamal Algorithm in 32-bit Computing System*. In: proceedings of the 3rd International Conference on Control, Automation and Systems Engineering. 2013: 1-5.

[5] Gamil R.S, Sanjay N.T. Encryption and Decryption of Digital Image using Colour Signal. *International Journal of Computer Science Issues*. 2012; 9(2): 588-592.

[6] Ismail A.I, Mohammed A, Hossam D. A Digital Image Encryption Algorithm Based on a Composition of Two Chaotic Logistic Maps. *International Journal of Network Security*. 2010; 11(1): 1-10.

[7] Singh P, Singh K. Image Encryption and Decryption using Blowfish Algorithm in MATLAB. *International Journal of Scientific and Engineering Research*. 2013; 4(7): 150-154.

[8] Kaladharan N. Unique Key using Encryption and Decryption of Image*. International Journal of Advanced Research in Computer and Communication Engineering.* 2014; 3(10): 8102-8104.

[9] Narendra K.P. Design and Analysis of a Novel Digital Image Encryption Scheme. *International Journal of Network Security & Its Applications*, 2012; 4(2): 95-108.

[10] Hung P.P, Naing T.M. A Novel Secure Combination Technique of Steganography and Cryptography. *International Journal of Information Technology, Modelling and Computing*. 2014; 2(1): 55-62.

[11] Challita K, Farhat H. Combining Steganography and Cryptography: New Directions. *International Journal on New Computer Architecture and their Applications*. 2011; 1(1): 199-208.

[12] Icox I, Miller M, Bloom J, Fridrich J, Kalker T. Digital Watermarking and Steganography, 2nd ed., Elsevier: Burlington, USA. 2008.

[13] Goeckel G, Vasudevan S, Towsley D, Adams S, Ding Z, Leung K. Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-hop Wireless Networks. *IEEE Journal on Selected Areas in Communications*. 2011; 29(10): 2067-2076.

[14] Kester Q. Image Encryption Based on the RGB Pixel Transposition and Shuffling. *International Journal of Computer Network and Information Security*. 2013; 7: 43-50.

[15] Shannon C.E. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949; 28(4): 656-715.

[16] Simon H. Communication Systems, 4th ed. John Wiley & Sons, Inc. New York. 2001: 742-749.

[17] Jaleel J, Thomas J.M. Guarding Image using Symmetric Key Cryptographic Technique: Blowfish Algorithm. *International Journal of Engineering and Innovative Technology*. 2013; 3(2): 196-201.

[18] Chaitanya P, Sree R. Design of New Security Symmetric and Asymmetric Cryptography Algorithms. *World Journal of Science and Technology*, 2012; 2(10): 83-88.

[19] Veerpal K, Anan S. Review of Various Algorithms used in Hybrid Cryptography. *International Journal of Computer Science and Network.* 2013; 2(6): 157-173.

[20] Anand K.M, Karthikeyan S. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. *International Journal of Computer Networks and Information Security*. 2012; 2: 22-28.

[21] Prasithsangaree P, Krishnamurthy P. Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs. *IEEE Gblobecom*. 2013: 1445-1449.

[22] Chehal R, Singh K. Efficiency and Security of Data with Symmetric Encryption Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2012; 2(8): 472-475.

[23] Marin G.A. Network Security Basics. *IEEE Security and Privacy*. 2005; 1(3): 68.

[24] Edney M. Real 802.11 Security: Wi-fi Protected Access and 802.11i. Addison Wesley Inc. New York. 2003; 7.

[25] Gunasekaran G, Mimal K.R. Encrypting and Decrypting Image using Computer Visualization Techniques. *ARPN Journal of Engineering and Applied Sciences*. 2014; 9(5): 646-650.

[26] Borie J.C, Puech W, Dumas M. *Encrypted Medical Images for Secure Transfer*. In: International Conference on Diagnostic Imaging and Analysis. Shanghai. 2002: 250-255.

[27] Upendra B, Shubhashish G. Analysis and Implementation of Selective Image Encryption Technique using MATLAB. *IOSR Journal of Computer Engineering*. 2014; 16(3): 108-111.

[28] Hayder R.H, Irtifah A.N. Image Encryption and Decryption in a Modification of Elgamal Cryptosystem in MATLAB. *International Journal of Sciences: Basic and Applied Research*. 2014; 14(12): 141-147.

[29] Sankaran K.S. Krishna B.V. A New Chaotic Algorithm for Image Encryption and Decryption of Digital Colour Images. *International Journal of Information and Education Technology.* 2011; 1(2): 137-141.

[30] Zhang Y, Liu W, Cao S, Zhai Z, Nie X, Dai W. *Digital Image Encryption Algorithm based on Chaos and Improved DES*. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. San Antonio, USA. 2009: 474-479.

[31] Jignesh R.P, Rajesh S.B, Vikas K. Hybrid Security Algorithm for Data Transmission using AES-DES. *International Journal of Applied Information Systems*. 2012; 2: 15-21.

[32] Adedeji K.B, Ponnle A.A. A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development. *International Journal of Scientific and Engineering Research*. 2014; 5(10): 804-811.

[33] Shika K, Ishank K. Data Security using RSA Algorithm in MATLAB. *International Journal of Innovative Research and Development*. 2013; 2: 479-481.

[34] Adedeji K.B, Ponnle A.A. Development of a GUI for Hybrid (DES-RSA) Data Encryption and Decryption for Transmission of Biomedical Data. *International Journal of Science and Research*. 2014; 3(11): 1281-1284.

[35] Aman K, Sudesh J, Sunil M. Comparative Analysis between DES and RSA Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2012; 2: 386-390.

[36] Samoud A, Cherif A. RSA Algorithm Implementation for Ciphering Medical Imaging. *International Journal of Computer and Electronics Research*. 2002; 1(2): 44-49