Cyber Warfare and Terrorism based on Data Transmission through Classical Cryptographic and Steganographic Algorithms

Victor Onomza Waziri, Ph.D., Idris Suleiman
Department of Cyber Security Science,
School of Information and Communication Technology,
Federal University of Technology,
Minna,
Niger Sate-Nigeria

ABSTRACT
The introduction of Internet has made it easier for everyone to access almost all information from different locations globally. This has made sensitive information prone to attack by malicious attackers. It therefore becomes important to come with measures that can be used to protect data on transmission from falling into wrong hands and to deliver some crucial messages surreptitiously especially at this age of political and religious cyber terrorism. In this paper, we propose a method of combining the features of cryptography and steganography to provide security to data in the Internet. We employ the techniques of vigenere cipher to scramble the message and then embed the encrypted message using the least significant bit method. The method provides confidentiality to information disseminations with the assumption that the adversary does not have the decrypting oracle mechanism.

Keywords
Stegnography, Vigenere Cipher, Confidentiality, Encrypted Message, Malicious Atackers

1. INTRODUCTION
Improvement in technology has led to the interconnection of systems globally. These systems are connected for the purpose of information exchange. Vital information's are transmitted over the information superhighways. The confidentiality, integrity and availability (CIA) (the basis of Information Security) of these pieces of information security are of serious concern to the users of these technological Internet layouts. Cryptography and Steganography are both used to provide security to information over the unsecure channel as they are on transmission over the ever busy communication traffic channel. Cryptography changes or scrambles the information from something meaningful to something gibberish in outlook to the adversary. Steganography hides the existence of the information by embedding it in communicating medium such as an image, audio, video and texts; this embedment could be on the surfaces or emerged in the aforementioned media that are technically called stego or surreptitious spaces of redundancies texts or images. Cryptography helps to provide secure communication through information encryption while steganography hides the information making it appear like no information is hidden in the object used (Phad, Bhosale and Panhalkar, 2012). The application of Cryptography and Steganography improves the message security; if the message is discovered, the gibberish may not be understood unless the adversary has a decryption oracle and it will take the adversary some asymptotic probabilistic polynomial time (PPT) to decrypt the message. These methods have much usage in computer related fields. They are used to protect confidential information to individuals and organization (Sumit and Amit, 2012) and this has weakened the aggressive information acquisition by fanatical religious terrorists and political adventurers from acquiring secret details of various political institutions over nations. This, however, has become a dirty channel in which political, black hackers and cyber terrorists are riding on the high crest of religious chauvinism to achieve their nefarious know-hows.

Cryptography techniques draw attacker's attention while steganography conceals the existence of the pieces of secret information on transmission. Stenographer's employ mostly images and texts to conceal the existence of their information (Sarabjeet and Sonika, 2013).

In this paper, we propose a hybrid of cryptographic and steganographic features to develop a model for secure data transmission that is fundamental secure against terrorism. The algorithm we are using for our encryption scheme is the well-known classical Vigenere encryption scheme. The encrypted data is later embedded into an image using the least significant bit techniques. The classical Vigenere cipher is a symmetric cipher that uses the same key for encryption and decryption. This cipher is harder to cryptanalyze as compared to other symmetric cipher because of the large key space that it possesses.

Our choice of classical cryptosystem is due to it none frequent application in the modern cryptographic computing utilities. That is, current institutions may not have developed decryption oracles to decrypt the stego when discovered based on trivial algorithmic encryption methods. In other words, cyberspace terrorism could best achieve its ends through unused classical cryptographic algorithms.

2. RELATED WORKS
In this section, we review some literatures that are based on related works.

Sarabjeet and Sonika (2013) proposed a method of using image steganography, the method is based on first component alteration using hybrid edge detector. RGB image edges were detected by hybrid edge detector which combines 3 x 3 matrixes scanning and Sobel edge detector. The result obtained revealed that high embedding capacity and image quality was achieved. An improved least significant bit based steganography for securing information was also proposed by Mamta and Parvinder (2013), an embedding algorithm for

concealing encrypted information in nonadjacent and random pixel locations in edges and smooth areas of images was presented. The information is first encrypted, the encrypted information is later embedded in an image by detecting edges in the cover image using improved edge detection filter. This method makes it difficult for eavesdroppers to know that information is being transmitted and formal steganalyses methods cannot break the stego image. Saleh (2013) proposed a method of combining cryptography and steganography to provide security to information. The information is encrypted using filter bank cipher and embedded using discrete wavelet transform. The combinations of these two methods provide a robust and strong system that is resilient to attack. The result obtains after computing the peak signal to noise ratio shows that the proposed system provides high performance. Kannaki, Porkodi, and Ananthi (2013) in their paper, developed a system that combines cryptography and steganography to provide confidentiality and security. The crypto graphical aspect of the system was achieved using advanced encryption standard and discrete cosine transform was used to implement the steganography aspect of the system. A highly secured method for data hiding was developed.

2.1 Cryptography

Cryptography is an area of science used to protect information either in storage or transit (Saleh, 2013). It is used to scramble sensitive information before transmission (Obaida 2013). The information is first scrambled or encrypted before storage or transmission and at the receiving end; the receiver decrypts the information (Saleh, 2013). There are three types of algorithm used in encrypting information in cryptography namely the symmetric, asymmetric and hash function (Phad, Bhosale, Panhalkar, and 2012). The symmetric techniques uses the same key for encryption and decryption, the asymmetric techniques uses different key usually called private and public key for encryption and decryption (Ayushi 2010) and the hash function uses a mathematical function to irreversibly encrypt information. Encrypted information is said to be secured if the cryptographic algorithm used is strong and the key can be kept secret from unauthorized persons. Different techniques for implementing cryptographic algorithms are available depending on what one wants to achieve. Cryptography provides some security services like confidentiality, integrity, access control, authentication and non-repudiation (Niveditha, 2014). Confidentiality ensures that information is viewed by only those who have the authorization to do so. The confidentiality aspect of it can be achieved using algorithm like the hill cipher, substitution cipher, Vigenere cipher, Caesar cipher, data encryption standard, advanced encryption standard among others that are more of modern encryption schemes. Integrity ensures that information are not modified (added to or deleted from) by those who does not have the permission to do so. Data integrity can also be monitored using massage digest 5 (MD5), SHA-1, SHA-5, SHA-3 among others. Authentication helps to verify the identity of two or more communicating systems. Non-repudiation ensures a system or user does not deny having any knowledge of the communication they initiated. Access control ensures the information is accessed by those who have the authorization.

2.1.1 The Vigenere Cipher

The Vigenere cipher is a polyalphabetic substitution cipher used to secure information. It is believed to be most effective and simplest (Ranju and Varghese 2014). It scrambles the information to be encrypted by using a key word usually called the key. It uses the 26 English alphabet for its operation (Rahmani,Wadhwa and Vaibhav 2012). For a keyword of length X, the number of possible keyword will be 26^X against cryptanalytic. The strength of the Vigenere cipher key depends on the length of the key and its secrecy. Because of the polyalphabetic nature of this cipher, it is more difficult to break. The repetitions of the key makes it vulnerable to attack (Ranju and Varghese 2014). The Vigenere cipher uses a table called the Vigenere table. The Vigenere table is a 26 x 26 matrix table used for substitution according to the different shift values derived from the key.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
W	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 1: The vigenere table (Rahmani,Wadhwa and Vaibhav 2012).

2.1.2 Algebriac Description

The encryption and decryption procedure for Vigenere cipher in mod26 can be represented algebraically as shown below

Let:

I = I1, I2, I3 . . . In be the information

C = C1, C2, C3 … Cn be the cipher text

K = K1, K2, K3 … Kn be the key space

E = Vigenere Encryption

D = Vigenere Decryption

EK (In) = (I1 + K) mod26 = Cn

DK (Cn) = (Cn - K) mod26 = In

2.2 Steganography

Steganography is the art of concealing information in such a way that prevents attackers from knowing that information is hidden in some undercover object. It involves hiding information using a suitable carrier like image, audio and/or video file (Mamta and Parvinder 2013). The stego image, audio or video can be transmitted across a public or an insecure channel without drawing attacker's attention. The main aim of steganography is to transmit sensitive information secretly by hiding its existence using image, audio and/or video (Payal, Ravimohan, and Sumit, 2013).Cryptography and steganography are related to each other as they both try to prevent unauthorized access to information. The major difference between them is that cryptography changes the information from something meaningful to something meaningless in the eye of an adversary while steganography embeds the information making it appear like no information is hidden at all (Mamta and Parvinder 2013). Like cryptography, they are different algorithm for implementing steganography. The algorithms include discrete cosine transform, least significant bits,

2.2.1 LSB Steganography

This is a widespread method used to embed images in texts. It changes the least significant bit in some bytes of the image in which information is to be embedded in to conceal a sequence of bytes containing the hidden data (Jayaram, Ranganatha, Anupama 2011). It is more efficient and effective for image steganography (Shilpa, Geeta and Neha, 2012). "In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd" (Jayaram, Ranganatha, Anupama 2011). The figure below shows how a word "HEY" can be hidden using the least significant method.

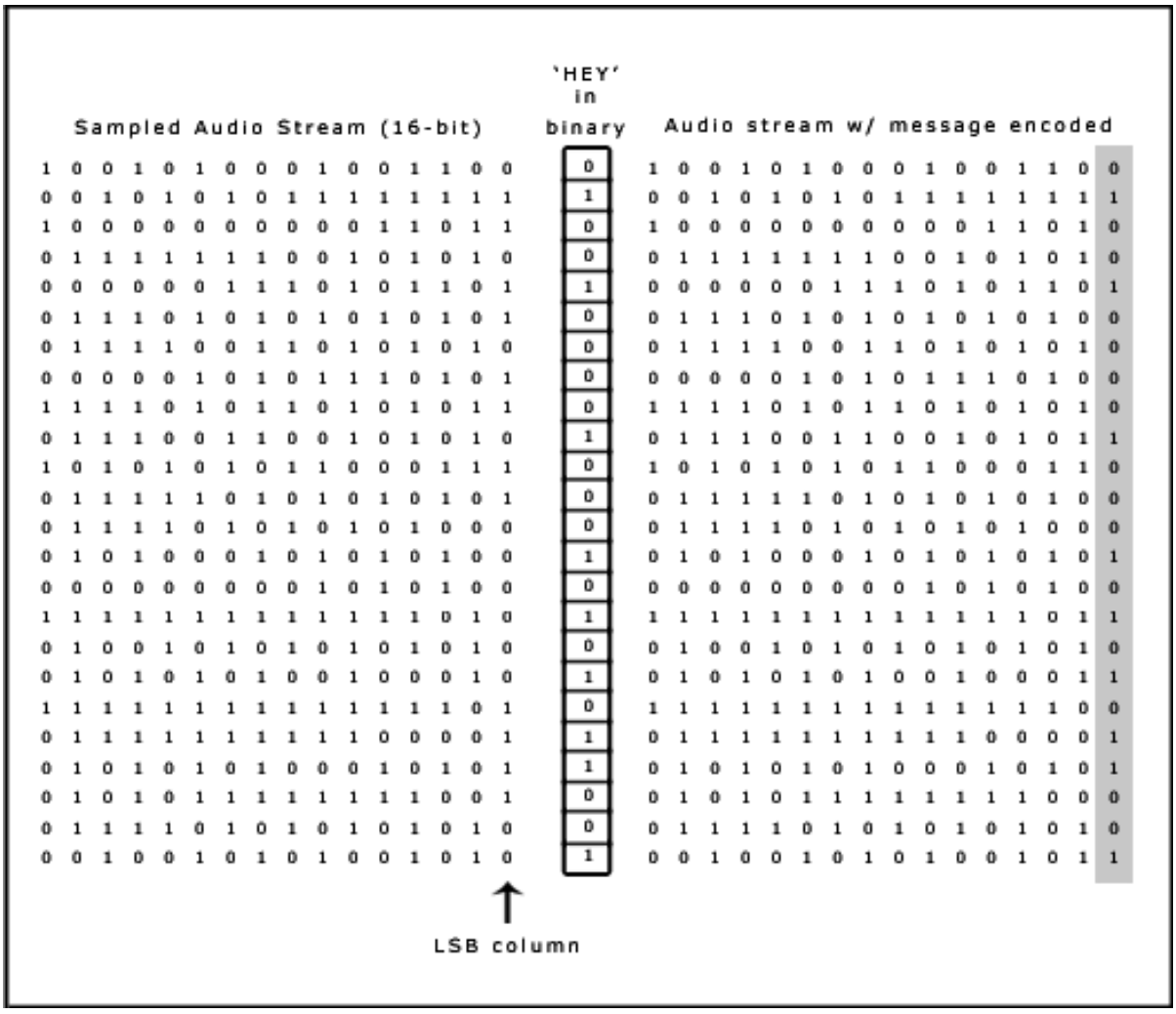
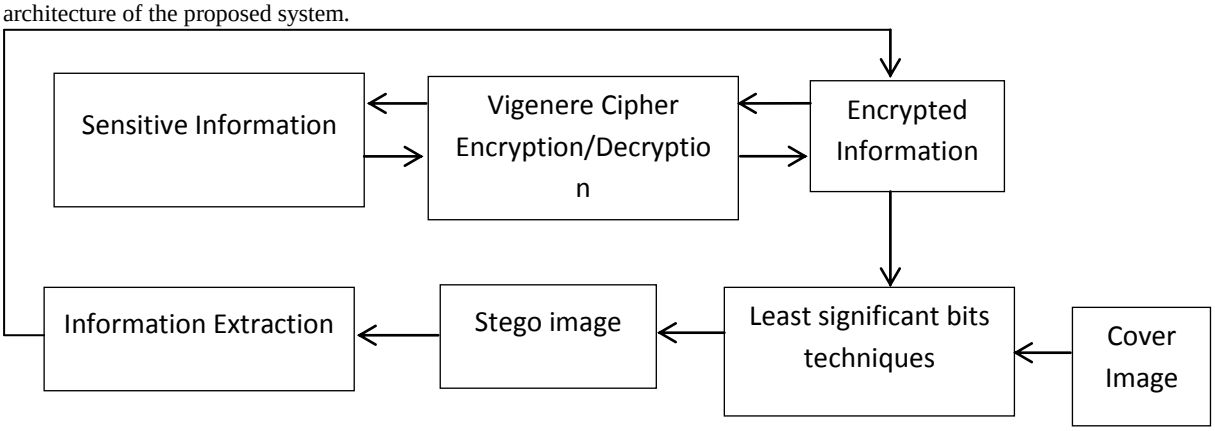


Fig. 2: LSB Example (Jayaram, Ranganatha, Anupama 2011).

3. METHODOLOGY OF THE PROPOSED SYSTEM

The proposed system combines the features of cryptography and steganography to provide security to information. The stego-image obtained can be freely transmitted without eavesdroppers knowing that a piece of information is being transmitted. The information to be transmitted is first encrypted using the Vigenere cipher and is then embedded in the least significant bit. The figure 3 below shows the block architecture of the proposed system.



3.1 Information Encryption and Decryption Procedure

The information to be transmitted is first encrypted using the vigenere cipher. The vigenere cipher works on the set of 26 english alphabet (Rahmani,Wadhwa and Vaibhav 2012). To encrypt the information, the user choses a keyword usually referred to as key. The longer the keyword the more difficult it will be to cryptanalyze. The method of generating the cipher text is described below.

Let:

Ek be the vigenere encryption

Dk the vigere decryption

Pi the plaintext or information

Ci the cipher text

Ki the key

The encryption of Pi is given as

Ek(pi) = (Pi + Ki)mod26

The decryption is Ci given as

Dk (Ci) = (Ci - Ki)mod26

For example to generate the cipher text for the plaintext SULEIMANANDDRWAZIRI, using the keyword CYBERSECURITY we follow the process described below

Ek (S) = (S+C) mod26 = (18 + 2) mod26 =

20mod26= 20 = U

Ek (U) = (U+Y) mod26 = (20+ 24) mod26 = 44mod26= 18 = S

Ek (L) = (L+B) mod26 = (11 + 1) mod26 =

12mod26= 12 = M

.Ek (I) = (I+S) mod26 = (8 + 18) mod26 =

26mod26= 0 = A

PLAINTEXT	S	u	l	e	i	m	a	N	a	n	d	d	r	w	a	z	i	r	i
KEYWORD	C	y	b	e	r	s	e	C	u	r	i	t	y	c	y	b	e	r	s
CIPHERTEXT	U	S	M	I	Z	E	E	P	U	E	L	W	P	Y	Y	A	M	I	A

3.2 Embedding Procedure

The second phase of the work is to embed the encrypted information. The cipher text is embedded using the least significant bit method. This method substitutes the least significant bits in the image with the bits of the encrypted information. the working process of this method is shown below.

Take the binary value of an image pixel as

10101101 10011011 01110101 10110110 01011010 01001111 11001010 10101010

To hide the letter “S” in this image using the LSB techniques. S has ASCII code value of 84 with the binary number 01010100

We substitute the least significant bit in each byte of the cover image with the bit of the message to be embedded. The outcome of this is as shown below

10101100 10011011 01110100 10110111 01011010 01001111 11001010 10101010

The difference between the stego image and the original image is not significant or noticeable to the human eye because of the high chances of the bits in the stego image being the same with the bits in the original image

4. EXPERIMENTAL RESULT

Using the images below (a logo and a car) as the cover image and the cipher text USMIZEEPUELWPYYAMIA generated using the vigenere cipher, we carry out the steganography using MATLAB and the following result were obtained

Fig 3: original image

Fig4: stego image

Fig.5 original image

Fig.6 stego image

The message was embedded and extracted successfully. They is no clear difference between the original image and the stego image in the human eye, therefore an eavesdropper will not be able to know that a message is embedded in the image.

5. CONCLUSION AND FURTHER RESEARCH WORKS

In this paper, we were able to hide a ciphertext using the Vigenere cryptosystem in an image stego under the platform of least significant bit method. We embed the encrypted message using MATLAB. The method provides data confidentiality as it scrambles the information and finally hides the existence of the message. The limitation of this system is that the message to be embedded would first be encrypted manually before embedding. Therefore, the longer the message the more time it will take to encrypt and decrypt even to the person who has the encryption and decryption key; thus, this has some semantic security embedded in the process. This means that until a decrypting oracle is applied on the stego, it be very difficult to cryptanalyze the message once the stego is obtained.

Classical algorithms could play more ingenious roles in in cyber warfare and terrorism in most cases, modern cryptography is concern with with developing advanced encryption schemes and the use of the classical schemes are not being harnessed into the modern encryption schemes.

With the advent of modern hacking in commercial institutions, religious bigotry, economy and political undercurrent activities in the International Cyberspace, we suggest more ingenious hybrid cryptosystems that involve both symmetric and public key encryption schemes based on some high probabilistic polynomial time that meets the standard of indistinquisability Chosen Cipher Attacks IND-CCA(1 or 2). Such cryptosystem schemes could be the combination of Rabin and AES cryptosystems that could involve confusion and diffusion processes.

6. REFERENCES

[1] Ayushi (2010). A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications, 1(15), 1-4

[2] Jayaram, P., Ranganatha, H. R., Anupama, H. S. (2011). Information Hiding Using Audio Steganography – A Survey. The International Journal of Multimedia & Its Applications,3(3), 86-96

[3] Kannaki, S.V., Porkodi, K.P., Ananthi M. (2013). Secure Data Hiding Using An Integration Of Cryptography And Steganography. Research Journal of Computer Systems Engineering,4, 558-563. Retrieved from: http://technicaljournals.org/RJCSE/

[4] Mamta Juneja and Parvinder S. Sandhu (2013). An Improved LSB Based Steganography Technique for RGB Color Images. International Journal of Computer and Communication Engineering, 2(4), 513-517

[5] Obaida, M. A. A. (2013). A New Approach for Complex Encrypting and Decrypting Data. International Journal of Computer Networks & Communications, 5(2), 95-103

[6] Phad, V. S., Bhosale, R. S., Panhalkar, A. R. (2012). A Novel Security Scheme for Secret Data using Cryptography and Steganography. I. J. Computer Network and Information Security, 2, 36-42 DOI: 10.5815/ijcnis.2012.02.06

[7] Payal, G., Ravimohan, and Sumit, S. (2013). A New Secure Encryption Algorithm Using Combination of Cryptography and Steganography. International Journal of software & Hardware Research in Engineering, 1(1), 73-76

[8] Saleh, S. (2013). A Secure Data Communication System Using Cryptography and Steganography. International Journal of Computer Networks & Communications, 5(3), 125-137

[9] Sarabjeet, K. and Sonika, J. (2013). Image Steganography using Hybrid Edge Detection and First Component Alteration Technique. International Journal of Hybrid Information Technology,6(5), 51-66

[10] Sumit, K., and Amit, K. (2012). Advanced Network Security Using Cryptography And Steganography. Journal of Global Research in Electronics and Communication, 1(1), 1-5,