International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 5, Issue 5, May 2016 **ISSN 2319 - 4847**

Multilevel secure image communication Based on (Cipher &Stegnography)and evaluation secure

Rasha Ibrahim Hussain.[1], Ashraf Gasim Elsid Abdalla.[2]

[1].Faulty of Telecommunication and Space Technology Engineering, Future University

[2.] School of Electronics Engineering Sudan University of Science &Technology, Khartoum- Sudan

ABSTRACT

With the revaluation of the information technology and the communication systems, the security of these systems has become a matter of concern. This paper tries to prototype a secure SMS system that relies on multilevel security, particularly a merge between LSB algorithm and the vernam. The purpose of the Vernam is to achieve the confidentiality; nevertheless the purpose of the LSB is to conceal communication. The evaluation of the Vernam based on m-sequence stream cipher was achieved by calculating the correlation coefficient in image case. The two stages implemented in Matlab. The result shows that the correlation coefficients in each case are very close to zero.

keywords:-Stegnography ,Vernam Logarithm , LSB , MSE , PSNR

1.INTRODUCTION

Recently, with the huge development of computers and communication services, most of organizations and formal communications are done by means of digital transactions and electronic communication systems. Clearly that is the reason why the security issue for those system transactions has become a matter of concern. One can define the computer security as: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information data, and telecommunications especially for those individuals and organizations at risk of security attacks breach. Those individuals or organizations could be military or civilians (such as trade companies, banks, and business people). "The security attack is defines as: any action that compromises the security of information owned by an organization" [1]. These risks led the scholars and designers of computer science and communication engineering to develop and implement secure communication systems for both private and public use. Those secure communication systems use one or more security mechanisms in order to achieve one or more security services. The security mechanism is defined as: the process (or a device whichincorporates such a process) that is designed to prevent, or recover systems form security attacks. Examples for the security mechanisms are cryptography algorithms, data integrity algorithms and authentication protocols. The security service is defines as: a processing or communication service that enhances the Security of the data processing systems andthe information transfers of an organization. These services are intended to avoid security attacks, and they make use of one or more security mechanisms to provide the service. Examples of security service: data confidentiality, data integrity, access control and authenticity [2]. Thus in order to achieve one security service, it requests one or more security mechanism. Our thesis proposes a merge between cryptography and steganography to provide data confidentiality and integrity for short message system (SMS). The fundamental objective of cryptography is enable people to communicate over an not secure channel in such a way that opponents cannot understand what is being said [3]. Steganography: The technical term itself is derived from the Greek words steganos thatmeans, “Covered” and graphia, which means “writing”. Steganography is the art of concealed communication [4]. The very existence of a message is secret [4]. The differencebetween steganography and cryptography simplified,is that cryptography techniques try to conceal the contents of a message, while steganography goes further to tries hiding the fact that a communication even exists [5]. We will design, implement and evaluate the performance of multilevel secure communication system. This system will send/receive a short encrypted message (image), covertitintoan innocent looking image. In thispaper wewill use the stream cipher based on secure pseudo random algorithm (ML algorithms) and LSB steganography algorithm.An engineer named Gilbert Vernam introduced Vernam stream cipher, his system based on binary data (bits), as the one time pad the length of the key is equal to length of the plaintext, thus the Vernam stream cipher is the stream cipher with key stream equal to the plaintext. The differences between the one time pad and Vernam are: the Vernam doesn’t require the true random generator in addition that the stream key couldbe used several times [1].

2.METHODOLOGY

methodology equation

Maximum length pseudo random bits generators (m sequence) Shift register based stream cipher

$$s_{m+1} = s_m p_{m-1} + \ldots\ldots\ldots\ldots + s_1 p_1 + s_0 p_0 \bmod 2$$

$$s_m = s_{m-1} p_{m-1} + \ldots\ldots\ldots\ldots + s_1 p_1 + s_0 p_0 \bmod 2$$

The next LFSR output can be computed as:

$$s_{m+1} = s_m p_{m-1} + \ldots\ldots\ldots\ldots + s_1 p_1 + s_0 p_0 \bmod 2$$

In general, the output sequence can be described as:

$$R_{xx}(k) = \sum_{i=0}^{L-1} X(i)X(i+k) \qquad s_{i+m} = \sum_{j=0}^{m-1} p_j . s_{i+j} \bmod 2; s_i, p_j \in \{0,1\}; i = 0,1,2$$

$$0 \le k \le L-1$$

M sequence definition

Math notation :Linear feedback shift register math illustration

$$r_{xx}(k) = \begin{cases} 1 \; for \; k = 0 \\ \dfrac{-1}{T} \; otherwise \end{cases}$$

$$where \; T \; ° \; period$$

Math notation: M sequence auto correlation function

Least significant bit algorithm

$$for \; i = 1, \ldots, L(c)$$
$$do$$
$$s_i \leftarrow c_i$$
$$end \; for$$
$$for \; i = 1 \ldots, L(m)$$
$$do$$
$$compute \; index \; j_i where \; to \; store \; ith \; message \; bits j_i \leftarrow cj_i \; m_i$$
$$end \; for$$

Algorithm: LSB cover

$$for \; i = 1, \ldots, L(M) \; do$$
$$compute \; index \; j_i, where \; the \; ith \; message \; bit \; is \; stored$$
$$m_i \leftarrow LSB(c_{j_i})$$
$$end \; for$$

Algorithm: LSB decover

Mathematic evaluation handles

In This part it show us the mathematical tools that will be used to evaluate the our performance

Autocorrelation

$$R_{xx}(\tau) = \int_{-T}^{T} x(t)\,x(t+\tau)\,dt \rightarrow (a)$$

$$R_{xx}(k) = \sum_{i=0}^{L-1} X(i)\,X(i+k) \rightarrow (b)$$

$$0 \leq k \leq L-1$$

Math notation :Autocorrelation function

Correlation coefficient

$$r_{xy} = \frac{cov(x,y)}{\sqrt{var(x)\,var(y)}}$$

$$var(x) = E(x - E(x))^2$$

$$= E(x^2 - 2xE(x) + E^2(x))$$

$$= E(x^2) - 2E^2(x) + E^2(x) =$$

$$\therefore var(x) = E(x^2) - E^2(x)$$

$$cov(x,y) = E[(x - E(x))(y - E(y)]$$

$$= E[xy - xE(y) - yE(x) + E(x)E(y)]$$

$$= E(xy) - 2E(x)E(y) + E(x)E(y)$$

$$\therefore cov(x,y) = E(xy) - E(x)E(y)$$

where

$E \equiv$ statistical expectation

$r_{xy} \equiv$ the correlation coefficient

$var \equiv$ statistical variance

$cov \equiv$ statistical coveriance

Math notation :Correlation coefficient continuous case

1. *let's* I and I' be 2-D discrete random variables with equal high m and with n. thus the correlation coefficient for these two variable is given as follow :

$$r(I,I') = \frac{\sum_{i,j}^{m,n}(I(i,j) - E(I))(I'(i,j) - E(I'))}{\sqrt{\sum_{i,j}^{m,n} I^2(i,j) - E(I)\sum_{i,j}^{m,n} I'^2(i,j) - E(I')}} \rightarrow (a)$$

where $E(I)$ is mean value

$$E(I) = \frac{\sum_{i,j}^{m,n} I(i,j)}{m\,n}$$

2. let R and R' *be* the 1-D discrete random variable whith equal length l. thus the correlation coefficient is given as follow .

$$r(R,R') = \frac{\sum_{i-1}^{l}(R(i) - E(R))(R'(i) - E(R'))}{l} \rightarrow (b)$$

where $E(R)$ is the statistical mean

$$E(R) = \frac{\sum_{i-1}^{l} R(i)}{l}$$

Mean square error(MSE):-
Math notation : Discrete random variable correlation coefficient

suppose $x = \{x_i \setminus i = 1, 2, \ldots\ldots N\}$ and $y = \{y_i \setminus i = 1, 2, \ldots\ldots N\}$ are two o finite length discrete signals, the MSE between the signal is

$$MSE(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2$$

in images case

suppose I, I' be the original and processed images respectively, then the MSE will given by the following equation

$$MSE(I, I') = \frac{\sum_{i}^{m}\sum_{j}^{n}(I(i, j) - I'(i, j))^2}{m\,n}$$

Math notation : MSE calculation
Peak signal to noise ratio (PSNR)

$$PSNR = 10\log\frac{L^2}{MSE}$$

where

L ≡ the dynamic rang of the original singal

MSE ≡ the mean square error between the orignal signal and the corrupted singal

Math notation : PSNR calculation
Image histogram

$h(r_i) = n_i$

where

r_i ≡ is ith gray level/shadow for example {0,1,…,255}

n_i ≡ is the number of pixels in the gray leve image/shadow matrix has r_i gray level/shadow.

Math notation :Image histogram calculations.

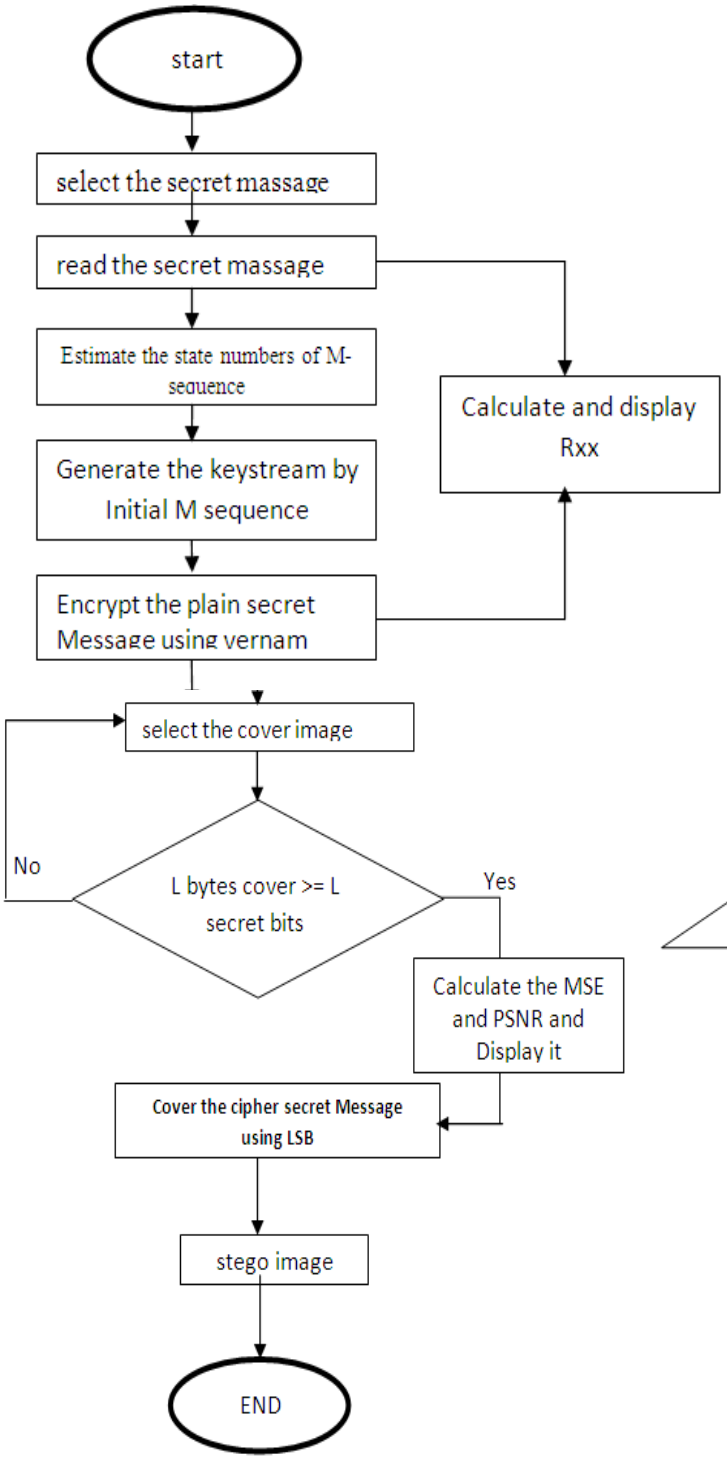
The algorithm applied LSB controlled by pseudo random number generators. The authors use the following procedures[6]:

- Both communication partners share a stego-key k usable as a seed for a random number generator.
- Then, they can create a random sequence k1, ..., kl(m) and use the elements with indices. Where l(m) is length of the secret message. In other works they generator a key stream with length equal to the message bits.
- Then, they will use the following bytes indices to hide the secret bit in the LSBs of each selected bytes (randomly selected).

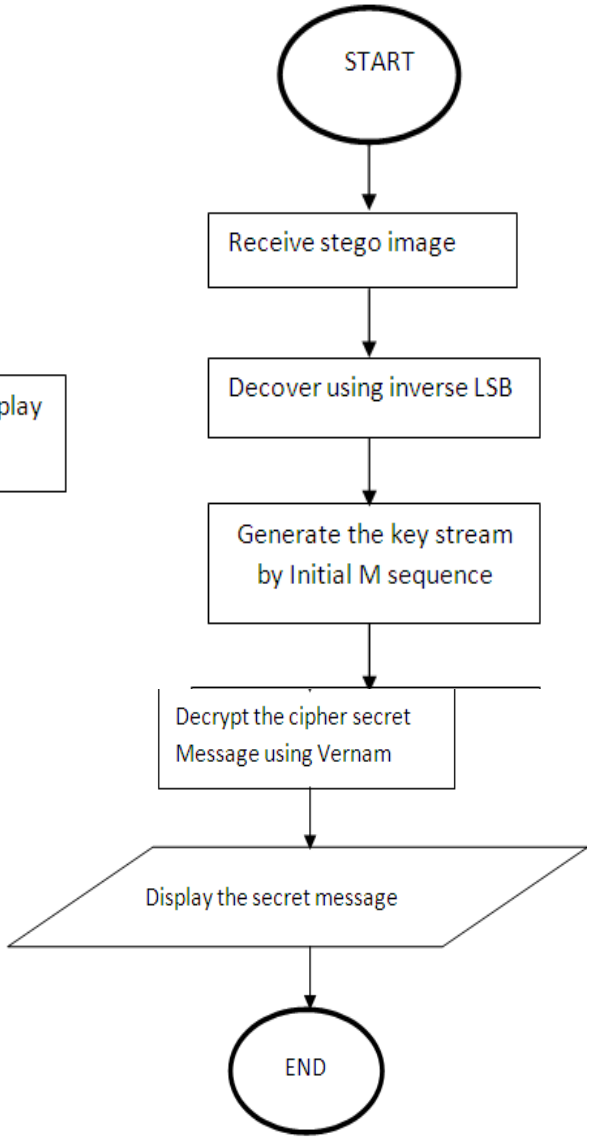
The authors said that provide high level of security because the secret information hidden in different position of LSB of covert image. The limitation of these methods underlying in it is still LSB. In the other words it is still pure steganography.

LSB and Vernam based on m-sequence combination theoretical advantages :-

- The combination is easy to implement in both hardware and software.
- Vernam based on m-sequence is more practical comparing to one time bad stream cipher.
- Vernam based on m-sequence is lighter than other well known stream cipher such as RC4. Because it only need piece of memory and clock generator.
- LSB is command steganography algorithm in use. Because it doesn't effect the visual semantic of the cover image.



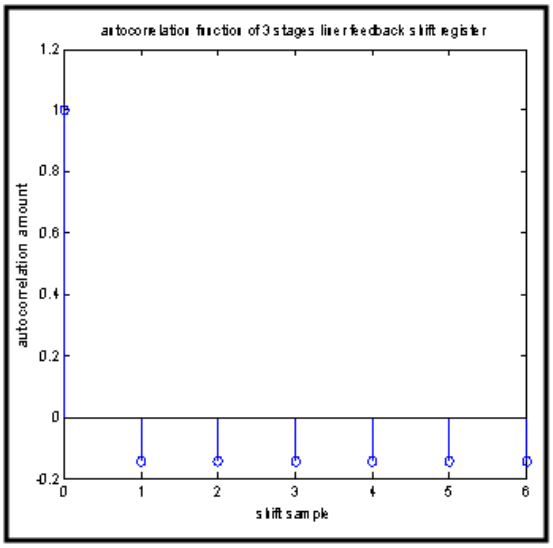
Sender flow chart



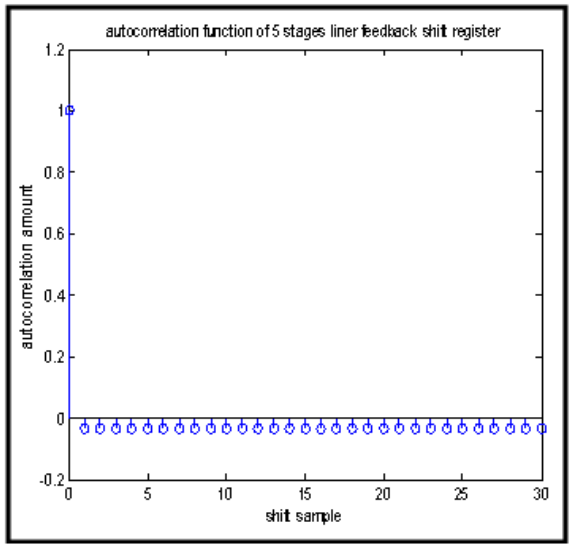
Receiver flow chart

3.EVALUATION RESULTS

We implement a function that can generate a maximum length pseudo random bits sequences (m-sequences). As mentioned earlier in this paper, the m-sequence must satisfy a certain qualification to consider as pseudo random bits generator. The figures from 5.2 to 5.4 illustrate the autocorrelation functions for 3, 5 and 7 states m-sequences respectively. Besides, the table(1) shows the number of zeros and ones for each 3, 5 and 7 states m-sequence.(testing result of our implement M-sequence gneration)



Figure(1): 3 Stages maximum length autocorrelation function



Figure(2) : 5 Stages maximum length autocorrelation function

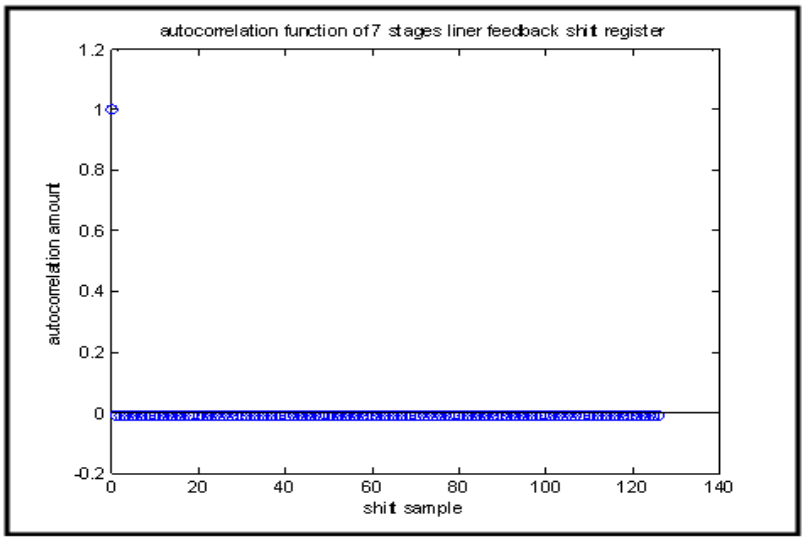


Figure (3): 7 Stages maximum length autocorrelation function.

Table(1) M-sequence testing results

Order of m-sequence(m)	Number of zeros	Number of ones
3	3	4
5	15	16
7	63	64

4.VERNAM ENCRYPTION ALGORITHM BASED ON THE M-SEQUENCE EVALUATION RESULTS.

The evaluation of Vernam stream cipher algorithm was done as follow:
Visualize the cipher message and the plain message (image).
Calculate the correlation coefficient between the cipher and plain message.
Visualize the image histogram for both encrypted and plain images.

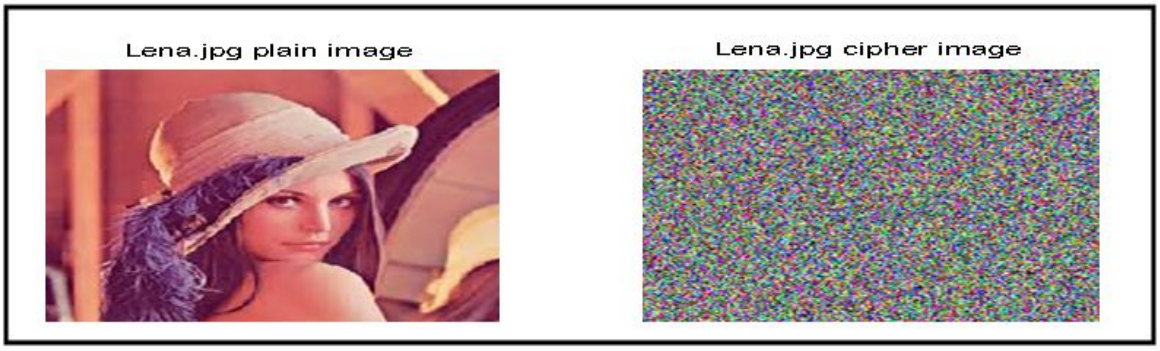


Figure (4) Image Encryption

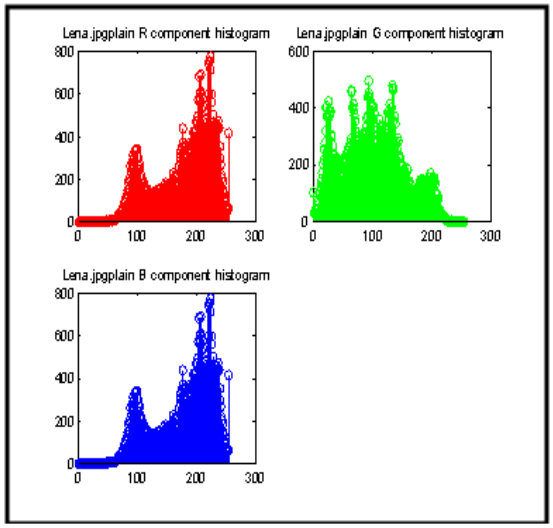


Figure (5) Lena plain/cipher image.

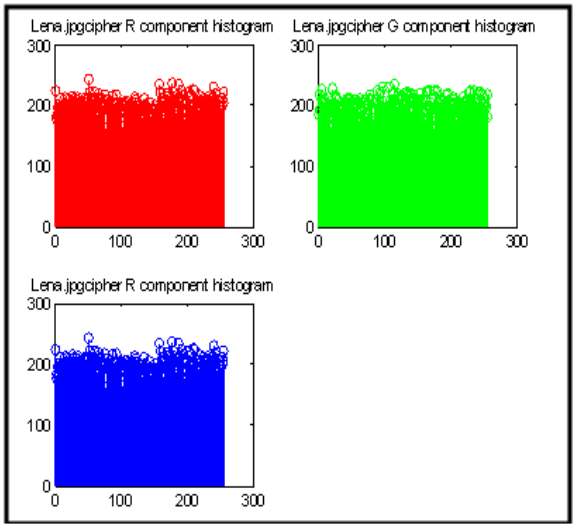


Figure (6) Lena plain image histogram.

Table (2) Image Encryption Result based on the m-sequence evaluation result

Image name	Size (Bytes)	Correlation coefficient
Lena	195075	0.000731021

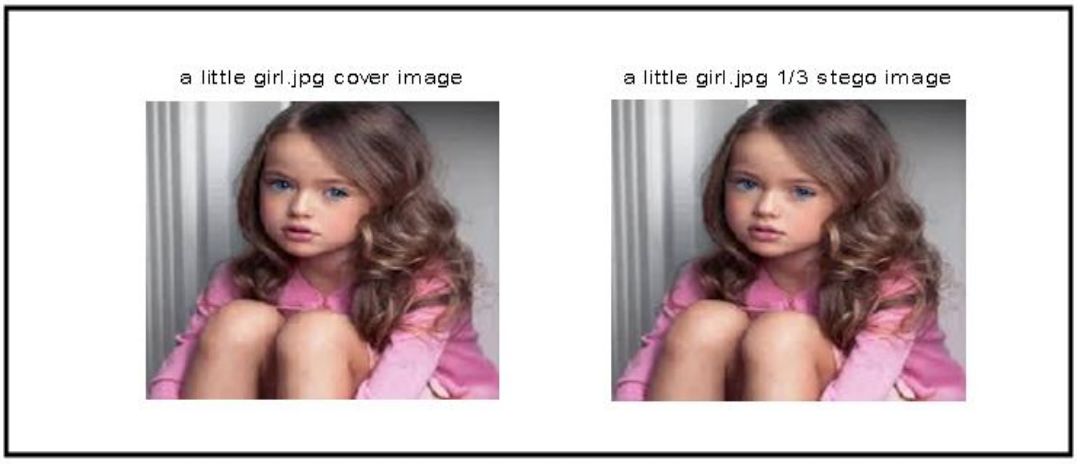
5.LSB EVALUATION RESULTS

The table shows the evaluation results of the LSB. And the figures to 5.16~5.22 show the cover images via its stegos. The table shows the results of MSE and PSNR for each image in the following case:

- 1/3 pay load (only 1/3 from the cover image used to embedding the secret using the LSB algorithm).
- 2/3 pay load (2/3 from the cover image used to embedding the secret using the LSB algorithm).
- Full pay load (the whole cover image used to embedding the secret using the LSB algorithm).
  - An embedding data are random data. Form the table, clearly the relationship between the pay load and the PSNR is opposite relationship. However the PSNR in the allowed limited that specified in [7].

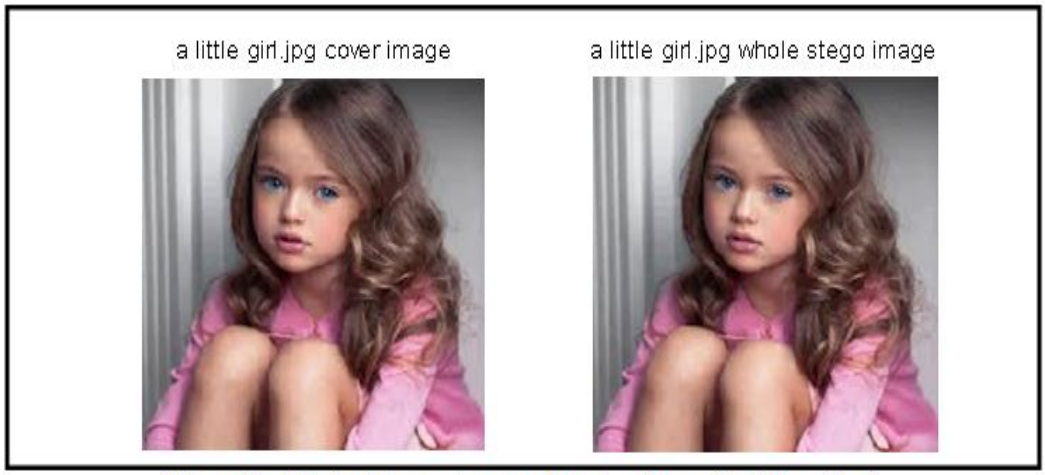
Table (3) shows the evaluation results of the LSB

Cover image		$\frac{1}{3}$ LSB for of cover		$\frac{2}{3}$ LSB for of cover		LSB whole cover	
Name	Size (byte)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
little girl	151074	0.1663	55.9213	0.3328	52.9096	0.4973	51.1642



Figure(7): A little girl cover image and its stego image for 1/3 pay load.

Figure(8): A little girl cover image and its stego image for 2/3 pay load.



Figure(9): A little girl cover image and its stego image for full pay load.

6.CONCLUSION

- From the evaluation results of the Vernam based on m-sequence stream cipher by mean of calculating the correlation coefficient for the (image). We realize that, the Vernam based on m-sequence stream cipher gives good correlation coefficients (they are very close to zero) independently from the type of the data. Implies, the cipher media in channel is almost unrecognized.
- Form the above point; it notice that, the conditional confidentiality almost achieved.

Hidden the encrypted data in the image and then send it, that done by LSB information hidden algorithm. That is trying to conceal the existence of the secret message in order to achieve communication concealing.

- The evaluation results of LSB algorithm induct that, the mean square error between the covert image and its stego is too small.
- As well as the MSE is too small, the peak signal to noise ratio (PSNR) is a good enough comparing to the standard one (28dB [7]) .

REFERENCE

[1]. William, Stallings, and William Stallings. Cryptography and Network Security, 4/E. Pearson Education India, 2006.
[2]. Stallings, William. Network security essentials: applications and standards. Pearson Education India, 2007.
[3]. Stinson, Douglas R. Cryptography: theory and practice. CRC press, 2005.
[4]. Cox, Ingemar, et al. Digital watermarking and steganography. Morgan Kaufmann, 2007.
[5]. Katzenbeisser, Stefan, and Fabien AP Petitcolas. "Information hiding techniques for steganography and Digial watermarking." Boston, London, Artech House (2000).
[6]. Prashanti, G., and K. Sandhyarani. "A New Approach for Data Hiding with LSB Steganography." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer International Publishing, 2015.
[7]. "fundamental of media security ". Wi Qi, Jonathan Weir &Ventus publishing Aps 2010. ISBN 978-87-7681-706-0.

Autthors brief Introudaction :-

Rasha Ibrahim Hussainis researcher in master level at future University-Sudan. she received master of Science (Msc) in data communication and network degree 2015 , she Received Bachelor Degree in Telecommunication Engineering degree in 2009 future University Research intersect are Mobile , satellite and Networks.

DrAshraf GasimElsidAbdalla,Associate Professor in Telecommunication Engineering and researcher in space technology center in future university.Also he is an academic members of electronic department in college of engineering, Sudan university of science and technology. Aformer lecturer and researcher in some Malaysian Universities
(UKM , UPM , UIA and MMU) . he got his PhD and M.Sc. from National university of Malaysia 2001 and 1996 in electrical and electronic system . He got his B.Sc. in electronic engineering from technical university of Budapest 1993. His researcher focus on Mobile and satellite Communication . He published more than 40 technical papers and supervised more than 50 Ph..D and master students.