Ciencia Digital
www.cienciadigital.org

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Mejora en la seguridad de un método estenográfico aplicando criptografía.

Improvement in the security of a Stenographic method by applying cryptography.

Raúl Cuzco Naranjo.[1], Carmen Mantilla Cabrera.[2], Byron Vaca Barahona.[3] & Rosa Acosta Velarde.[4]

Recibido: 08-03-2017 / Revisado: 12-05-2017 Aceptado: 05-06-2018/ Publicado: 01-71-2018

Abstract.

The objective of this research was to present a proposal to improve the security of messages transmitted in images based on the Least Significant Bit (LSB) steganographic method, and incorporating the César cryptographic algorithm of great compatibility with LSB since the alteration is not visible of the steganographed image and the message is only decipherable for the receiver. The method was implemented in a web application developed with Java Netbeans, the images were compared with Guiffy Image Diff and the data integrity was verified with the HashMyFiles tool. An increase in the security level of 76.67% was obtained when applying the proposal in the case study, it is recommended to carry out the experiment with other cryptographic algorithms.

DOI: https://doi.org/10.33262/cienciadigital.v2i3.137

Keywords: Steganography in Images, Cryptography, LSB, Cipher of Cesar, telematics Security.

[1] Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Riobamba, Ecuador, rcuzco@espoch.edu.ec
[2]Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Riobamba, Ecuador, carmen.mantilla@espoch.edu.ec
[3]Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Riobamba, Ecuador, bvacab@espoch.edu.ec
[4] Escuela Superior Politécnica de Chimborazo, Facultad de Administración de Empresas, Riobamba, Ecuador, rosa.acosta@espoch.edu.ec

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Resumen.
El objetivo de esta investigación fue presentar una propuesta de mejora en la seguridad de mensajes transmitidos en imágenes, basada en el método esteganográfico Least Significant Bit (LSB), e incorporando el algoritmo criptográfico César de gran compatibilidad con LSB ya que no existe visible la alteración de la imagen esteganografiada y el mensaje solo es descifrable para el receptor. El método se implementó en una aplicación web desarrollada con Java Netbeans, se compararon las imágenes con Guiffy Image Diff y se verificó la integridad de datos con la herramienta HashMyFiles. Se obtuvo un incremento en el nivel de seguridad del 76.67 % al aplicar la propuesta en el caso de estudio, se recomienda realizar el experimento con otros algoritmos criptográficos.

Palabras Claves: Esteganografía en Imágenes, Criptografía, LSB, Cifrado de Cesar, Seguridad Telemática

Introducción .

Los ataques de los hakers son cada vez más sofisticados, las empresas se vuelven más vulnerables pues se expone la seguridad de su información privilegiada (Inteco, 2012), debido a esto es prioritario implementar métodos de seguridad para preservar la confidencialidad e integridad de datos compartidos como secretos comerciales o lanzamientos de nuevos productos. La esteganografía ofrece un gran potencial para reducir el riesgo de fuga, además de mejorar la privacidad individual en la comunicación. Aunque no es un sustituto para la criptografía, la esteganografía proporcionando seguridad y privacidad (Díaz, 2010).

Esta técnica de ocultar mensajes dentro de un medio multimedia (Reza, 2017), en conjunto con métodos de comunicación permite realizar intercambios ocultos de información de tal manera que no se sospeche que lleva almacenada información. Hoy en día existen varios métodos esteganográficos que permiten ocultar información dentro de distintos tipos medios digitales como: imágenes, sonido y video pasando desapercibidos, al momento no existen procesos de seguridad en el análisis al enviar la imagen esteganografiada.

Varias investigaciones se enfocan en cifrar y ocultar mensajes utilizando diversas técnicas o métodos. Saini y Verma (2013) en su trabajo proponen un método de cifrado eficiente para asegurar las imágenes en color multimedia. Se utilizan respuestas dinámicas complejas de múltiples sistemas caóticos de orden superior para llevar a cabo los procesos de barajado y difusión de los píxeles de imagen bajo el control de la clave secreta. Los resultados de la simulación validan que el método propuesto tiene un gran rendimiento de cifrado y practicabilidad.

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

De la misma manera, Jung y Yoo (2014), en su investigación proponen un método de ocultación de datos semi-reversible que utiliza la interpolación y la técnica de sustitución menos significativo. En donde en primer lugar, los métodos de interpolación se utilizan para aumentar la escala de la imagen y la cubierta hacia abajo antes de ocultar los datos secretos para una mayor capacidad y calidad. En segundo lugar, el método de sustitución LSB se utiliza para incrustar datos secretos. Los resultados de esta investigación destacan como ventaja la capacidad de transmitir gran cantidad de información manteniendo su alta calidad visual. Una de las desventajas es que no se pudo mejorar la seguridad durante la transmisión.

De la revisión de literatura realizada en este trabajo se evidencia que no se ha aplicado criptografía para mejorar la seguridad en la transmisión de información oculta en imágenes, por tal razón, este trabajo tiene por objetivo, el desarrollo de un método esteganográfico que incorpore técnicas criptográficas a fin de mejorar la seguridad de los mensajes transmitidos dentro de una imagen, fortaleciendo de esta manera la seguridad de la información en caso de que sea interceptada. A más de eso se pretende dar a conocer en el campo de la esteganografía mediante el uso de un software desarrollado en este trabajo para este método.

El trabajo presenta como primera fase un estudio de métodos esteganográficos en imágenes y algoritmos criptográficos. A continuación, la propuesta del nuevo método esteganográfico con criptografía es implementado en una aplicación web desarrollada con Java Netbeans, tomó como base LSB ya que permite alterar cualquier bit del byte de la imagen para ocultar el mensaje, se combinó con el cifrado de Cesar por su compatibilidad con este método esteganográfico pues no genera grandes cambios visuales en la imagen.

Se estructuró un caso de estudio cuya población tiene la característica de poseer conocimientos de criptografía y seguridad informática, esta población se ve reflejada en los estudiantes de quinto semestre de la carrera de Ingeniería en Sistemas pues cumplen estos rasgos, se dividió en un grupo de control y otro experimental a los cuales se les aplicó un diseñó de tareas para obtener el mensaje secreto sin y con el método propuesto para determinar la mejora en la seguridad del mensaje transmitido en la imagen. Finalmente, se presentan los resultados obtenidos de los mismos y las conclusiones de la investigación.

Metodologia.

Con la esteganografía se puede insertar un mensaje de forma segura dentro de un medio de multimedia como audio, video, imágenes y otros, de tal manera que esta información solo pueda ser recuperada por un usuario legítimo que conozca el método determinado de extracción de la misma. (Villagrán, 2002; Perea, 2012, Iglesias, 2014). Existen numerosos métodos esteganográficos, el más común es el de ocultar información dentro de una

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

imagen, por lo que se realizó un análisis, exponiéndose sus ventajas y desventajas como se presenta en la Tabla I (Reza, 2017).

Tabla 1. Ventajas y desventajas de Métodos Esteganográficos

Método esteganográfico	Ventajas	Desventajas
Patchwork	Utiliza la distribución Gaussiana, la información se esconde en forma de parches aleatoriamente.	Oculta muy poca información y para ocultar la información se debe tener registrado donde se encuentra la información para su recuperación.
Codificación por textura de bloques	Busca regiones con patrones similares entre la imagen y la información a ocultar.	Es realizado necesariamente por un operador humano quien se encargara de escoger las regiones fuente y destino.
Codificación de tasa de bits elevada	Está diseñada para tener un mínimo impacto en la percepción de la imagen. Existe un mayor control sobre las imágenes.	Es muy sensible sobre las modificaciones en la imagen.
LSB(Bits menos significativo)	Tiene una alta tasa de bits de inserción tiene una baja complejidad computacional	Poca robustez
Codificación de fase	Las modificaciones en las fases permiten tener una transmisión encubierto de información	Nivel medio de robustez, si la trasmisión sufre un ataque, la información no se recuperar en su totalidad.

Elaborador por: Grupo de Investigación.

Una vez analizada las ventajas y desventajas de los métodos esteganográficos se propone realizar con el método LSB puesto que tiene una tasa de bits baja y no solamente se puede insertar en el último bit, sino que también se puede insertar en cualquier bit del byte, la alteración de la imagen es mínima por no decir nula y el mensaje se encuentra insertado a lo largo de sus pixeles, se realiza en las áreas más ruidosas donde no atrae la atención (López, 2012). Con respecto a la complejidad computacional se logra mejorar su robustez con el nuevo método planteado para así convertirle en una fortaleza con el nuevo método planteado.

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

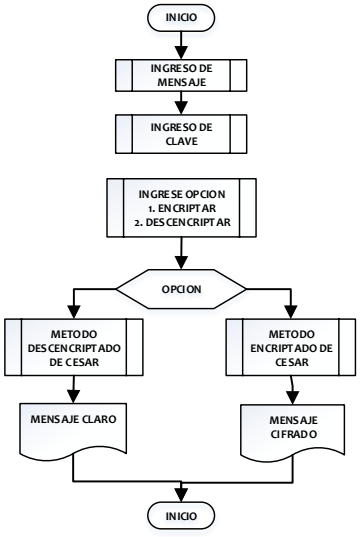
La importancia de la criptografía radica en que la información que lleva sea ilegible para la persona a la que no fue dirigida, pero el remitente puede descifrarla (Galende, 1995). Los métodos criptográficos pueden ser clásicos pueden ser por transposición o de sustitución, el primero cifrar el mensaje, cambiando simplemente el orden de las letras mediante algún patrón y el de sustitución consiste en reemplazar las letras del mensaje original por otras.

Existen algunas técnicas de cifrado por sustitución como la matriz de Polibio Changir, 2017), cifrado de Playfair y cifrado de Cesar, este último presenta una simplicidad y compatibilidad con el método LSB. Cesar es una técnica muy simple, donde cada letra del mensaje se mueve un determinado número de espacios en el alfabeto, logrando así un nuevo mensaje cifrado, mientras mayor sea el número de espacios a recorrer en el alfabeto mayor es el nivel de seguridad (Lucena, 1999).

Criptografia en el metodo esteganografica en imágenes.

Para la mejora en la seguridad del método esteganográfico LSB en imágenes se propuso implementar uno nuevo unificando con el cifrado de Cesar debido a la gran compatibilidad pues no altera la imagen al momento de insertar el mensaje encriptado. La Figura 1 se ilustra el proceso de encriptación/des-encriptación implementado con el cifrado de Cesar para asegura el mensaje a ser transmitido.

Figura 1. Diagrama de encriptación y desencriptación de mensaje



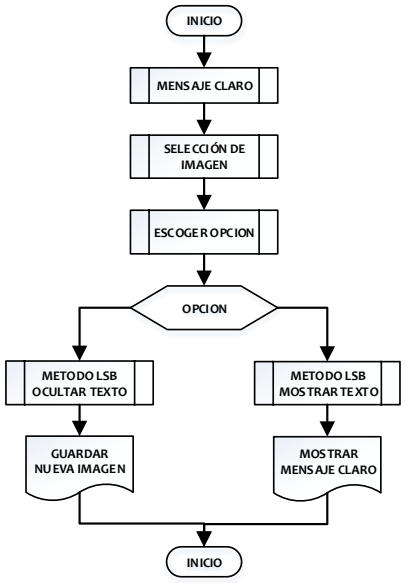
Elaborador por: Grupo de Investigación.

En síntesis, la propuesta de método consiste en selección de imagen a utilizar, ingreso de mensaje a ocultar, entrada del número clave para el proceso de encriptación del mensaje, ejecución del algoritmo César, ejecución del algoritmo esteganográfico LSB y creación de

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

la nueva imagen con el mensaje oculto. La Figura 2 muestra el diagrama de flujo para ocultar/mostrar el mensaje encriptado en una imagen esteganografiada.

Figura 2. Diagrama ocultar/mostrar mensaje encriptado



Elaborador por: Grupo de Investigación.

Este proceso se desarrolló por medio de una aplicación desarrollada en Java con Netbeans. Los parámetros establecidos por el usuario antes del ocultamiento del mensaje en la imagen son: el número de desplazamientos a aplicar en el cifrado de Cesar, el mensaje que se desea modificar y la imagen selecciona para ocultarlo, esta puede estar en formato Windows BitMap (BMP), Graphics Image Format (GIF), Joint Photographic Experts Group (JPEG), Tagged Image File Format (TIFF), Portable Network Graphics (PNG), ya son los más utilizados ya que la aplicación lo permite (García, 2004).

Se comparó las imágenes pixel a pixel con Guiffy Image Diff, lo que permitió determinar los cambios realizados en las componentes de cada pixel, se verificó la integridad de los datos ejecutando la herramienta HashMyFiles y con la aplicación esteganografía básica disponible en la web se pudo obtener el mensaje esteganografiado.

Se validó la propuesta a través de un caso estudio, donde los sujetos de prueba tienen conocimientos de Criptografía y Seguridad Informática lo que constituye nuestra población, estas características cumplen el grupo de estudiantes de quinto semestre de la carrera de Ingeniería en Sistemas, se dividió la población en un grupo experimental y uno de control. Se diseñó un conjunto de tareas y se les pidió extraer el mensaje oculto en una imagen esteganografiada, el experimento se realizó con el método para el grupo experimental y sin el método propuesto para el grupo de control, se permitió utilizar cualquier tipo de herramientas de criptoanálisis y estegoanálisis.

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Se establecieron niveles de seguridad, el nivel alto indica el número de estudiantes que no pudieron mostrar el mensaje claro oculto dentro de la imagen por el lapso de 2 horas que duró la prueba, el nivel medio indica el número de estudiantes que lograron mostrar el mensaje claro en un tiempo de una hora y 45 minutos del tiempo y el nivel bajo indica el número de estudiantes que mostraron el mensaje claro en un tiempo de una hora con 30 minutos.

Resultados.

La Figura 3, muestra el mensaje obtenido con la aplicación Esteganografía Básica antes de encriptarlo, como se puede observar el mensaje es legible, además se ve que la aplicación no presenta algun sistema de seguridad.

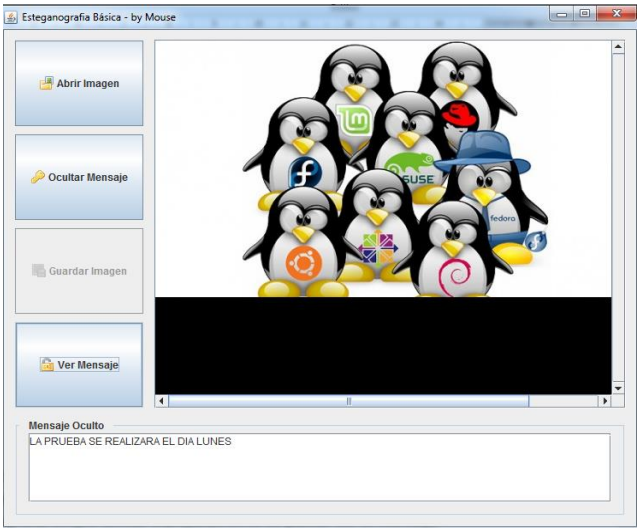


Figura 3. Captura del mensaje transmitido antes de aplicar la propuesta
Fuente: Esteganografia Básica

En la Figura 4 se presenta la interface desarrollada del método propuesto, obsérvese los parámetros a ingresar para ese proceso.

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Figura 4. Interface desarrollada de esteganografia con criptografia
Fuente: Autores

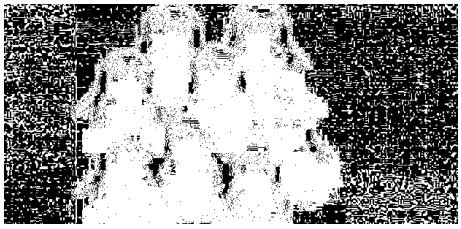
En la Figura 5, se puede evidenciar que el mensaje transmitido con el nuevo metodo propuesto no es legible aunque sea interceptado, ya que se encuentra encriptado.

Figura 5. Captura del mensaje transmitido después de aplicar la propuesta
Fuente: Esteganografia Básica

En la Tabla II se observa la comparación pixel a pixel de las imágenes original y esteganografiada con Guiffy Image Diff donde se marcaron los pixeles cuyos componentes fueron modificados, pero a simple vista la alteración no es visible.

Tabla II. Comparativa de imágenes

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018



Pixeles modificados

Imagen sin texto oculto

Imagen con texto oculto

Verificación de la integridad del mensaje transmitido con el método propuesto.

Una vez receptado el mensaje se aplicó el programa HashMyFiles para verificar el MD5 (código único de un archivo que indica cambios en una imagen), en la Figura 6 se puede observar que este código es el mismo tanto el archivo del emisor como del receptor, por ende, el archivo no ha sufrido ningún cambio.

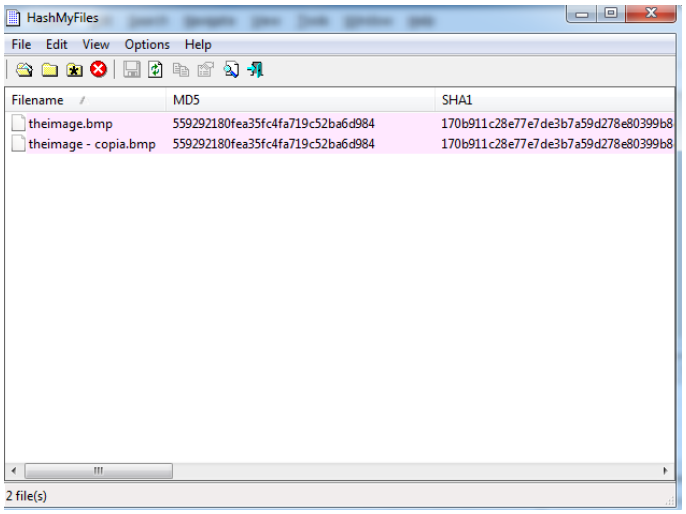


Figura 6. Verificacion de MD5
Fuente: HashMyFiles

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Validación del método.

La población de estudio fue de 60 estudiantes, se dividió en dos grupos de 30 estudiantes una para el grupo de control y el otro para el experimental. Al finalizar las pruebas en la tarea para obtener el mensaje transmitido, en el grupo de control los 30 estudiantes descifraron el mensaje. Al aplicar el nuevo método al grupo experimental se obtuvieron los resultados que se presentan en la Tabla III, como se puede observar 23 estudiantes no obtuvieron el mensaje, esto representa un 76.67 % de mejora en la seguridad para obtener el mensaje respecto al grupo de control.

Tabla III. Nivel de seguridad en el mensaje con el método propuesto

Nivel Seguridad	Nº Estudiantes
Alto	23
Medio	5
Bajo	2

Fuente: Autores

Conclusiones.

De la revisión de literatura se evidencia que LSB es uno de los métodos esteganográficos de imágenes más utilizados, presenta ciertas debilidades, pero se toma como base para la mejora pues tiene características que permiten no solo ocultar siguiendo un patrón, sino que se puede seguir otras opciones como alterar en cualquier otro bit del byte logrando así otra forma de ocultar el texto dentro de la imagen.

Del estudio se determinó que de los diversos algoritmos criptográficos que existen, el cifrado de Cesar tiene gran compatibilidad con LSB, en las pruebas realizadas se observó que no hay cambios visibles en la imagen. Pero mientras mayor sea la dificultad del algoritmo esteganográfico a implantar mayor va hacer el nivel de seguridad de la información.

En el caso de estudio el 100% del grupo de prueba pudieron obtener el mensaje oculto de la imagen sin el método propuesto, y al realizar la misma tarea con la aplicación del método propuesto en el grupo experimental solo siete estudiantes pudieron descifrarlo, lo que demostró que se incrementa el nivel de seguridad en un 76.67%.

Del estudio de herramientas esteganográficas disponibles se evidenció que el método propuesto en la aplicación desarrollada presenta la característica inusual para encriptación lo que le hace una herramienta confiable y robusta mejorando el nivel de seguridad en la transferencia de imágenes en cualquier formato.

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Referencias bibliográficas.

David García Cano. (2004). *ANÁLISIS DE HERRAMIENTAS ESTEGANOGRÁFICAS*. UNIVERSIDAD CARLOS III DE MADRID, MADRID. Recuperado a partir de http://e-archivo.uc3m.es/bitstream/handle/10016/7119/PFC_David_Garcia_Cano_2004_201033204919.pdf?sequence=1

Inteco. (2012). Recuperado a partir de http://www.expresionbinaria.com/el-arte-de-ocultar-informacion-esteganografia/

Eulins Changir, H., Hernandez. (2017). METODOS DE CIFRADO Y POLITICAS DE SEGURIDAD. Recuperado 18 de febrero de 2017, a partir de http://loshermanosiutll.simplesite.com/

Díaz Vico, Jesús (2010). *Esteganografia y EstegoAnalisis: Ocultación de Datos en STREAMS DE AUDIO VORBIS*. Universidad Politecnica de Madrid, Madrid.

Galende, C. (1995)**.** *La criptografía medieval*. Recuperado 1 de marzo de 2017, a partir de http://pendientedemigracion.ucm.es/info/citechar/jornadas/II%20JORNADAS/jor02galende.pdf

Jung, K.-H., & Yoo, K.-Y. (2014). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications*, *74*(6), 2143-2155. https://doi.org/10.1007/s11042-013-1832-y

Manuel López Michelone. (2012.). Esteganografía: para cifrar mensajes en imágenes. *unocero*. Recuperado a partir de https://www.unocero.com/2012/11/28/esteganografia-para-cifrar-mensajes-en-imagenes/

Jesús Villagrán. (2002.). Orígenes de la esteganografía. *VSantivirus*. Recuperado a partir de http://www.vsantivirus.com/esteganografia.htm

Pablo F. Iglesias. (2014). #MundoHacker: Esteganografía, el arte de ocultar información sensible. Recuperado 1 de marzo de 2016, a partir de http://www.pabloyglesias.com/mundohacker-esteganografia/

Paz Álvaro. (2014.). Herramienta para realizar técnicas de esteganografía y estegoanálisis. *Herramienta para realizar técnicas de esteganografía y estegoanálisis*. Recuperado a partir de http://www.gurudelainformatica.es/2014/08/herramienta-para-realizar-tecnicas-de.html

Perea, S. (2012, diciembre 7). Esteganografía: fotografías con firma invisible. Recuperado 25 de febrero de 2016, a partir de http://www.xatakafoto.com/tutoriales/esteganografia-fotografias-con-firma-invisible

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Saini, J. K., & Verma, H. K. (2013). A hybrid approach for image security by combining encryption and steganography (pp. 607-611). IEEE. https://doi.org/10.1109/ICIIP.2013.6707665

Lucena López, Manuel José. (1999). Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. Edición virtual. España. 1999. http://www.kriptopolis.org

Victor Reza. (2017). ESTEGANOGRAFIA. Recuperado 19 de febrero de 2017, a partir de https://prezi.com/8lp4ji-qayyu/esteganografia/

ISSN: 2602-8085
Vol. 2, N°3, p. 61-73, Julio - Septiembre, 2018

Para citar el artículo indexado.

Cuzco R., Mantilla C., Vaca B. & Acosta R. . (2018). Mejora en la seguridad de un método esteganografico aplicando criptografía. *Revista electrónica Ciencia Digital* ***2***(3), 61-73. Recuperado desde: http://cienciadigital.org/revistacienciadigital2/index.php/CienciaDigital/article/view/137/122