Using RC6 in embedding information in spatial parts of image construction

Shaymaa AbdulHussein Shnain [1], May A. Salih [2] , Baydaa Jaffer AlKhafaji [3]
Math and Computer Science Department, Basic Education College, University of Babylon, Hilla1
Email :shaymaahusain2015@gmail.com
Math and Computer Science Department, Basic Education College, University of Babylon, Hilla2
Email: may.abd@uobabylon.edu
Computer Science Department College of Education for Pure Science/ Ibn Al-Haitham University of Baghdad, Iraq3
Email : bayda.khafaji@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: With the development of means of communication, computer science and information exchange via electronic information networks an urgent need emerged to find ways to save exchanged information Encryption had a prominent role in this area However, with the development of intrusion hackers become able to access to information and change it This showed the need to adopt more sophisticated technology and more confidentiality in order to preserve the information So, it become famous to use the system of coverage in which the sent the information being invisible to anyone, through hiding it inside the sent media, such as audio, image, text, and video The purpose of this research is to maintain the security and confidentiality of information against a hacking operation Or break the image code as it is a cryptographic application where it encrypts images Which we want to keep from tampering with the intruders, and that the image to be encrypted is robust BMP 24bit This paper deals with how the key is generated and then uses it to encrypt

The selected image opens this code with the same key and this process was executed by language Programming MATLAB This paper aims to apply the idea to hide image message, using the least significant bi t algorithm inside an image and encrypt it in a new way for encryption .For the purpose of increasing security of the access of the letter it is being encrypted to hide the message before using the Encryption for the highs text This in turn increases the strength of encryption .

Keywords: JPEG,TIFF ,**PBM, PICT**, PCD, PCT.

Introduction

Become aware of information security place of great interest by researchers those interested in those who are trying to get the solutions and techniques of new and updated to ensure the protection of the information send and receive across the worldwide Web of information (Internet) without the occurrence of any breach or revealed by actors. It was to be keep up with the development of security information and create techniques and sophisticated hence the afternoon of knowledge hide information and development of the adoption of technology concealment The technique concealment of the methods of protection that make me sending and receiving invisible, in order to hide messages certain inside cover specific. Aim achieved the process of concealment is not to exciting any point doubt the existence of data hidden, while the goal analyst concealment is a doubt in all messages posted, and checked to make sure that the presence of data hidden where. Called a process that is where an attempt to a party detect the presence of the information hidden or read or change or delete the process of decoder concealment So I figured I needed to find a means of a multi-purpose of receipt of information and data properly and protected from informed of the third-party is authorized to access to this information [6] [5] appeared aware of encryption is science, which means methods which processed concerned the protection of store information and transfer in the field of a wide, and these methods depend on the secret key is used to encrypt the data. Although encryption is a good way to protect information, it is easy to detect and can be manipulated by any intruder. The need for more sophisticated, more confidential and data-intensive technology, especially with the emergence and evolution of the Internet, Seeing data as encrypted is enough to push a hacker or attacker to believe that important or sensitive data exists in random or encrypted text. It starts by using anti-encryption techniques to try to obtain its content. Even if it fails to do so, it may tamper with or distort it or use some means Available To prevent their access to their goal [4]. The major and major challenge faced by the information security field is the emergence of computer networks and means of communication in order to store, enter and provide information internally within organizations and externally from and to remote host systems. A new term has been added to the Information Security Glossary, Network Security, which is defined as the correct protection of all components associated with the computer network, including data, communication tools and infrastructure.

DIGITAL IMAGE

An image may be defined as a two-dimensional function f (x , y) where x and y are spatial (plane) coordinates, and the amplitude of (f) at any pair of coordinates is called the intensity of the image at that point. The term gray level is used often to refer to the intensity of monochrome images Color images are formed by a combination of individual images. For example, in the RGB color system a color image consists of three individual monochrome images, referred to as the red (R), green (G), and blue (B) primary (or component) images.

Type of digital image

BINARY IMAGE

A binary image is represented by an m*n logical matrix where pixel value are 1(true) or 0(false).

GRAYSCALE

A grayscale image m pixels tall and n pixels wide is represented as a matrix of double data type of size m*n elements values denote the pixel grayscale intensities in [1,0]

TRUE COLOR IMAGE

A true color RGB image is represented as a three dimensional m*n*3 double matrix each pixel has red , green , blue components along the third dimension with value in [1,0]

Header files

A header usually starts with some sort of unique identification value called a file identifier, file ID, or ID value. Its purpose is to allow a software application to determine the format of the particular graphics file being accessed. BMP, PCX, JPEG, FLI/FLC, and AVI files include headers that define the image size, number of colors, and other information needed to display the image. Fast graph provides functions for reading the image headers and retrieving their more useful items

IMAGE EXTENSION

GIF (Graphic Interchange Format) files use a maximum of 256 colors, and are best for displaying non continuous-tone images or those with large areas of flat colors, such as navigation bars, buttons, icons, logos, or other images with uniform colors and tones.

PNG (Portable Network Group) file format is a patent-free replacement for GIFs that includes support for indexed-color, grayscale, and true-color images, and alpha channel support for transparency. PNG is the native file format of Macromedia Fireworks MX. PNG files retain all the original layer, vector, color, and effects information (such as drop shadows), and all elements are fully editable at all times. Files must have the png file extension to be recognized as PNG files by Macromedia Dreamweaver MX. 0

JPEG (Joint Photographic Experts Group) file format is the superior format for photographic or continuous-tone images, because JPEG files can contain millions of colors. As the quality of a JPEG file increases, so does the file size and the file down load time. You can often strike a good balance between the quality of the image and the file size by compressing a JPEG file.

TIFF : tagged image file format

PBM: portable bitmap file format

PICT: picture file format

PCD: photo cd file format

PCT : picture format

PIF : program information file format

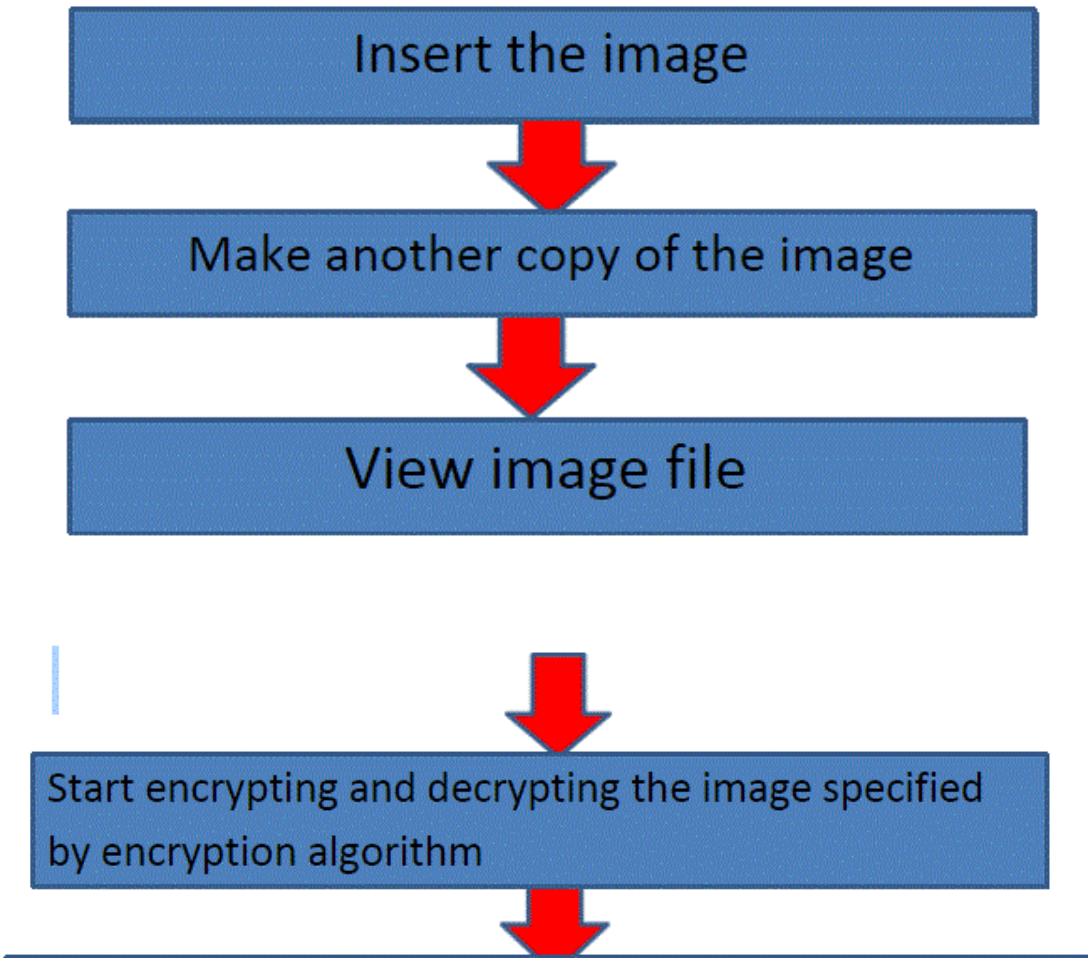
PIT : macintosh packlt format

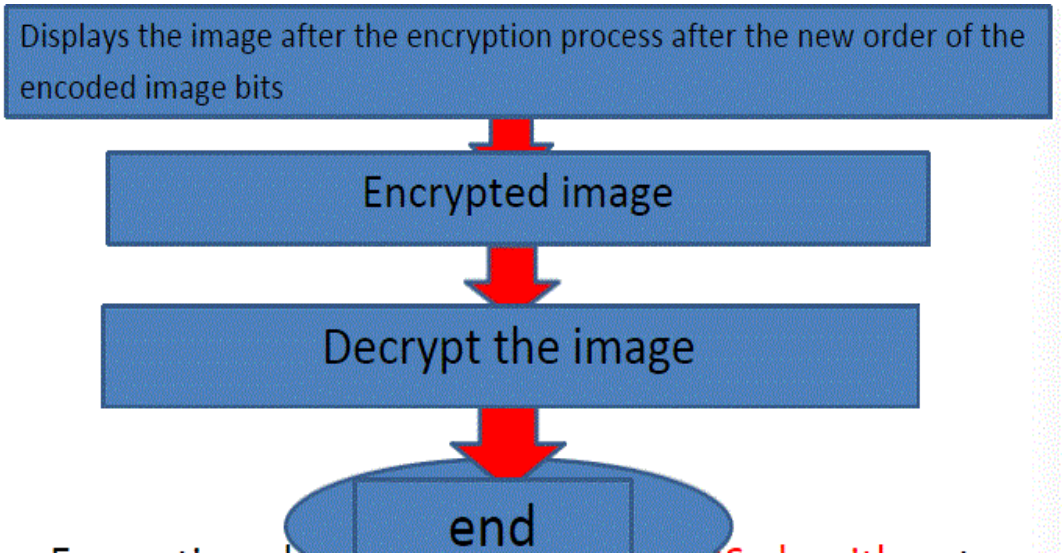
PNT :mac paint format

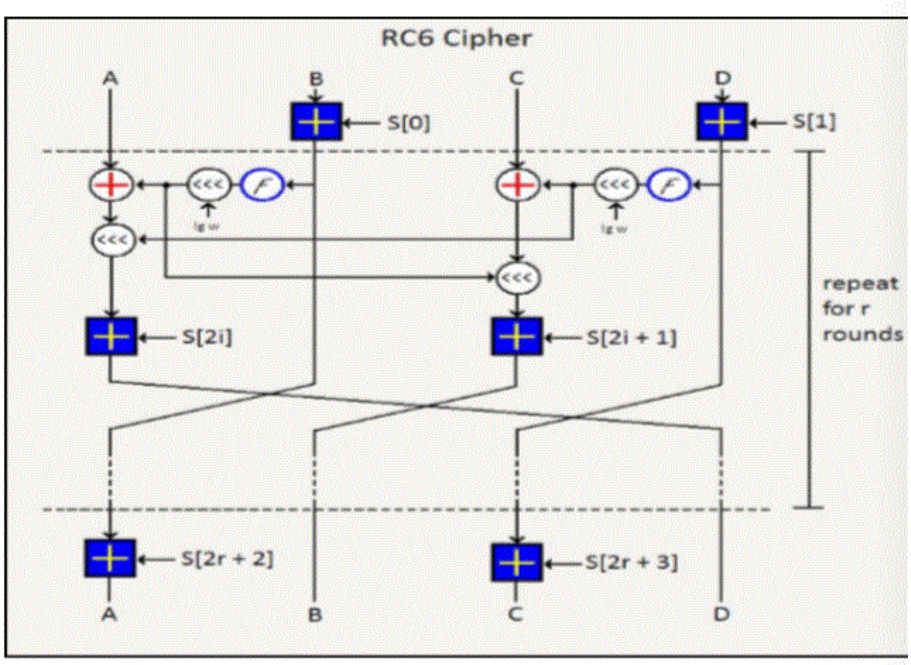
General encryption algorithm:

The cryptographic algorithm is a general image of a cryptographic algorithm The text is different in handling since the image file is treated differently from Text file, where the encryption process in the image focuses on encrypting bits for each pixel This is done by mixing these bits with the specific encryption algorithm we produce Pixels are scattered and unintelligible and thus perform the required work which is to get The image is encrypted and the meanings are not clear and thus the security and confidentiality of the image is maintained Tampering

The following line shows the process of encrypting the image in a detailed and clear format







Encryption algorithm was used is RC6 algorithm to encrypt the image This algorithm works on the image data of bits for all image pixels where A, B, C, D This algorithm divides the set of these bits into four clusters and then performs complex operations on those bits as we explained earlier The following diagram represents the encryption algorithm RC6 Encryption in this algorithm goes through several stages where we can summarize the work of this algorithm in the next steps

1_ input block data (128 bit size)
The block is divided into four parts A, B, C, D each part is 23 bits

2_ Enter the encryption key and its size is also 128 bits, and starts its S [0, ... 2r + 3].

2_1_ take the first part B and do the first steps of encryption, where we take part B and we merge the segment with the key S [0] and the following equation: 2_2_ B = B + S [0] The result obtained from step (1_2) Function f, and this function performs complex operations on that result where you add a specific statement to the key or cluster or both to increase the intensity of the complexity can be explained by the following equations: Key = hash (password + salt)
For 1 to 65000 do 3_2_ We take the result from step (2_2) and then perform the displacement of three orders according to the following equation: t=(B(2B+1))<<<1gw

Note: We convert the result from step (3_2) to section C as shown in Fig

3_We do the same before but this time between the two parts c, d where we take d and combine it with the key s [1] The same processes are performed in terms of scaling and function f but with different equations As we observe in the following equations
u =((D (2D+1)) <<< lgw
C=((C ^ u) <<< t) + S[2i+1]

Note: These steps are repeated at each session until the number of courses passed by the algorithm is 10. Courses

4_The final results obtained from this algorithm are as follows

C D B C A B D A

Note: In order to decrypt, we follow the same steps in the opposite way (ie, reverse encryption).

Conclusions:

In light of the results of this study can be inferred Encryption has an important role in maintaining data security from hackers Keep confidential data private The decryption process retrieves the encrypted image into a standard image Recommendations I recommend using encryption to prevent unauthorized access to data and personal images For the development of the project can be added to the cover of the image in addition to the process of encryption to make the image more secure.

References:

1. Owens, M., “A discussion of covert channels and steganography”, SANS Institute, 2002
2. Jamil, T., “Steganography: The art of hiding information is plain sight”, IEEE Potentials, 18:01, 1999
3. BJ AlKhafaji, MA Salih, S Shnain, Z Nabat,segmenting video frame images using genetic algorithms,2020 Periodicals of Engineering and Natural Sciences1114-1106 ,(2) 8
4. BJ AlKhafaji, M Salih, S Shnain, Z Nabat ,improved technique for hiding data in a colored and a monochrm images,2020, Periodicals of Engineering and Natural Sciences1010-1000 ,(2) 8
5. AL-Khafaji, B.J. Image Improvement Using The Combination of Wavelet and Multiwavelet Transform. *Ibn Al-Haitham Journal For Pure And Applied Science*.**2010**, *23*, *3*, 275-282.
6. Al-Khafaji, B.J. DetectTheInfected Medical ImageUsing Logic Gates. *Ibn Al-Haitham Journal For Pure And Applied Science*.**2014**, *27*, *2*, 260-267.
7. R.C. Gonzales and R.E. Wood: *Digital image processing*,second edition, prentice hall, 2002.
8. K. Belkacem-Boussaid and A. Beghdadi, “Non Linear Smoothing Method Based on the Just-noticeable Contrast,” IEEE Conference, pp. 843-847, 2005.
9. T. –L. Ji, M. K. Sundareshan, and H. Roehrig, “Adaptive Image Contrast Enhancement Based on Human Visual Properties,” *IEEE Transactions on Medical Imaging*, Vol. 13, No. 4, December, pp.573-586, 2008.
10. Proceedings of 2nd Singapore International Conference on ImageProcessing 2000.