Large Amount of Data GIF Image Encryption with High Security using Path-based Animation

Hind Rostom Mohammed
University of Kufa College of Mathematical &Computer Sciences/Computer Dept.
hind_restem@yahoo.com

. Ebtesam Najim Abdullah
University of Kufa

Informatics Center for Research and Rehabilitation

Ebtesamnajim@yahoo.com

Ameer Abd Al-Razaq University of Kufa Computer Center

ameer19842003@yahoo.com

Abstract

This study deals with constructing and implementing new algorithm based on hiding a large amount of data (image, audio, text) file into color GIF image. We have been used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly with Path-based animation rather than sequentially using new concept. This concept based on both visual and statistical that defined by main cases with there cases for each byte in one pixel. High security layers have been proposed through multi layers to make it difficult to break through the encryption of the input data using RC6 algorithm. The proposed algorithm can embed efficiently a large amount of data that has been reached to 86% of the image size with high quality of the output.

The proposed method depended on two factors: First, the image which is containing the encrypted text, this image is GIF type which is the abbreviation of (Graphics Interchange Format Image), and the Second factor is the text targeted by encryption and entering within the image.

Keywords: Graphics Interchange Format Image, Encryption, Flash Card, Internet, Information Transfer.

1-Introduction

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. In digital world, the security of digital images becomes more and more important since the communications of digital products over open network occur more and more frequently, movement is actually made up of many frames. Image encryption plays a significant role in the field of information hiding. It is argued that the encryption algorithms, which have been originally developed for text data, are not suitable for securing many real-time multimedia applications because of large data sizes. Software implementations of ciphers are usually too slow to process image and video data in commercial systems. Hardware

implementations, on the other hand, add more cost to service providers and consumer electronics device manufacturers.

Animation is the rapid display of a sequence of images of artwork or mode l positions or frames in order to create an illusion of movement. Animation starts with independent pictures and puts them together to form the illusion of continuous motion. In animation jargon, each image is called a frame [1].

An object seen by the human eye remains chemically mapped on the eye's retina for a brief time after viewing. This phenomenon is called persistence of vision. The human mind needs to conceptually complete a perceived action. This phenomenon is called phi. Usually, movies will run at 25 to 30 fps but computer animations can run at 12 to 15 fps.

Anything less than 12fps will be jerky motion as the eye is able to detect the changes from one frame to the next.

GIF (Graphics Interchange Format) is Image format that is widely used on the World Wide Web, both for still images (palletised color raster images) and for animations. The GIF format is particularly suited to rendering images that contain large blocks of the same color, or large blocks of repeating patterns. Additionally, it does not suffer from the lossyness that leaves JPEG unable to display flat, clean, color without losing all compression. Therefore, whenever a logo is seen on the internet, chances are that it is a GIF [2].

A very useful advantage of the .GIF format over the newer ones is the support for animations. One of the versions GIF is allows for a short sequence of images to be stored within a single file, which brings on the animation effect on the computer screen. One of the main reasons for the GIF image file format to be less used today is the Unisys patented data compression algorithm called LZW it is based on.

The proprietary nature of GIF requires that it is distributed through image-handling software only under strict licensing conditions. In GIF Image animation, the frame GIF Images (every pixel of each frame) are first loaded into the system memory and are then rapidly displayed on the screen from the memory. GIF Image animation takes huge amount of memory since all pixel information is to be first loaded into memory.

In vector animation, the images for each frame are calculated and generated by the computer. Vector animation takes up lesser memory space, but more time is generally needed to create the images than to load them from memory or disk.

In this research, we collect the information of the text from the encrypted image using very good algorithm of encryption to send through the internet to recipient.

The process of analyzing and encrypting the image can be divided into two parts: (i) determining start points at each encrypted text included within the image and letting the algorithm start with which to help us secure transferring message process. These separated encrypted texts are best symbolized within the image by point- like vector at equivalent distances then comes the process of (ii) embodying the original image points within the encrypted texts. After that it will be transferred through a coordinated format agreed upon with recipient so he can reformat it in their correct format after receiving it, therefore all deviated points are excluded due the "text noise" which is attached to the image data [3].

Experiments shows more reliance on the suggested method for improving the exactitude of the encryption process in the same time keeping the original data of the target image , this suggested method over comes the problem of having defects of code

easy decoding and regarding the problem of inaccurate recognition between the included images data and included text .

2- Common Techniques of Animation:

There are three techniques of animation [4]:

(A) Keyframe Animation

Historically, the animator has to create every frame of an animation by hand. Depending on the quality, one minute of animation might require between 720 and 1800 separate still images. Each frame in an animation reflects small changes from the previous frame. The master artists by having them draw only the important frames, called key frames. Junior animators or assistants could then draw the frames that were required in between the key frames. The in-between frames are called tweens [5].

(B) Path Animation

Moves an object along a pre-determined path-straight line or curve on the screen. Object does not change although it can be resized or reshaped. The tweening motion is an example of path animation-key frames (starting point and the destination point) are set and the program does the in-betweening for you.

Tweening: process of generating intermediate frames between two images to give the appearance that the first image evolves smoothly into the second image.

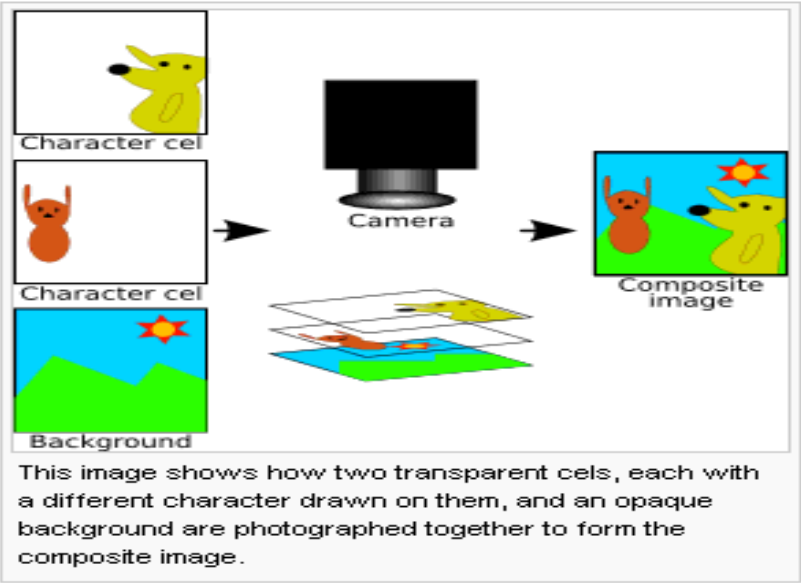
Animated GIFs Sequence of images can be stored in a single GIF file, and displayed one after another by a Web browser or other software

There is no browser plug-in can specify looping and delay between frames, 256 color palette and no sound [6]. Fig.(1) shows the path animation.

(C) Cel Animation

Cel comes from the word celluloid (transparent sheet material) used to draw the images and place them on a stationary background. The background does not change but the object does, example of the cel animation shown in Fig. (2).

Figure (1): Path Animation.



This image shows how two transparent cels, each with a different character drawn on them, and an opaque background are photographed together to form the composite image.

Figure (2): Composite Image.

Table (1): RC6 Algorithm Encryption and Decryption.

RC6 Algorithm Encryption	RC6 Algorithm Decryption
Encryption: Plain text stored in four w-bit input registers A, B, C, D	Decryption :Cipher text stored in four w-bit input registers A, B, C, D

B = B + S [0]
D = D + S [1]
for i = 1 up to r do
{
t = (B X (2B + 1)) <<< lg w
u = (D X (2D + 1)) <<< lg w
A = ((A t) <<< u) + S [2i]
C = ((C u) <<< t) + S [2i+ 1]
(A, B, C, D) = (B, C, D, A)
}
A = A + S [2r + 2]
C = C + S [2r + 3]
	C = C – S [2r + 3]
	A = A – S [2r + 2]
	for i = r down to 1 do
	{
	(A, B, C, D) = (D, A, B, C)
	u = (D X (2D + 1)) <<< lg w
	t = (B X (2B + 1)) <<< lg w
	C = ((C – S [2i + 1]) >>> t) u
	A = ((A – S [2i]) >>> u) t
	}
	D = D – S [1]
	B = B – S [0]

result will appear in the text tab after decoding [2], see Table (1).

The design of RC6 is more complex than that of RC5, and consequently an analysis of the cipher gets more involved [4]. The security of RC6 relies on the strength of data-dependent rotations, the mixed use of exclusive-or operations and modular additions, and on the squaring function f together with the fixed rotation squaring function f together with the fixed rotation [3]. Fig. (3) Shows the design of RC6.

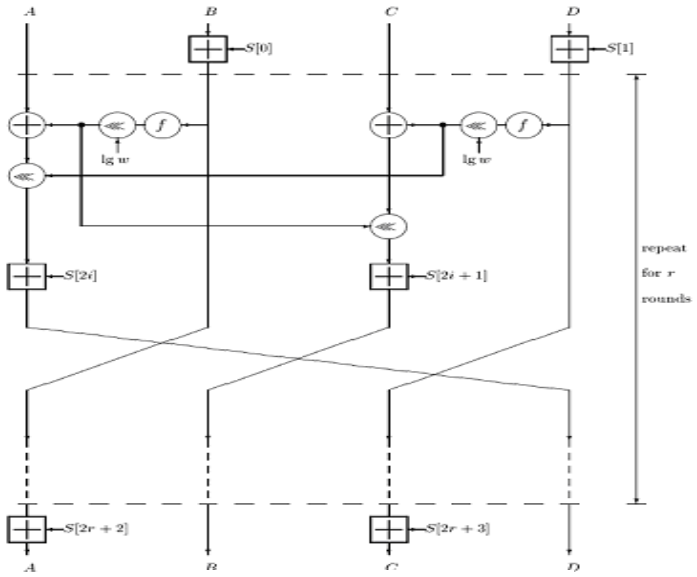


Figure (3): Diagram of RC6 [6].

3- Application of RC6 for Digital Images

A text message securely transferred by hiding it in a digital image file. 128 bit AES encryption is used to protect the content of the text message even if its presence were to be detected. Currently, no methods are known for breaking this kind of encryption within a reasonable period of time. Additionally, compression is used to maximize the space available in an image [5]. To send a message, a source text, an image in which the text should be embedded, and a key are needed. The key is used to aid in encryption and to decide where the information should be hidden in the image; another image or a short text can be used as a key. To receive a message, a source image containing the information and the corresponding key are both required. The

We use the GIF image-horse of size 140*60 plain text size (164 char) and RC6-32/20/16 are used. Figure (4) show six state for horse image motion for original image, Figure (5) show the results of RC6 block cipher for horse sub image (15*15) in both encryption/decryption digital images successfully. Also, it reveals its effectiveness in hiding the information in both encryption/decryption contained in them. In this paper, the plaintext that wants to be encrypted put it inside part of the selected image. The part of the image which is the heel of the right leg, where has been used to put the text inside the image after encrypt and merge the data of the part of the image with the data of the encrypted text in order to be transformed via internet by an E-mail letter . The algorithm RC6 was applied on the plaintext to be encrypted. Then the encrypted data were put and merged with the data of the selected part .Figure (6) illustrates the encrypted text.

Six shots were taken to the chosen part as illustrated by the Figure (5). The data of the sub image that selected from the original image are changing after each motion of the horse's body and can be illustrated in the Table (2): The results of the encryption/decryption in sec. are illustrated in Table (3).

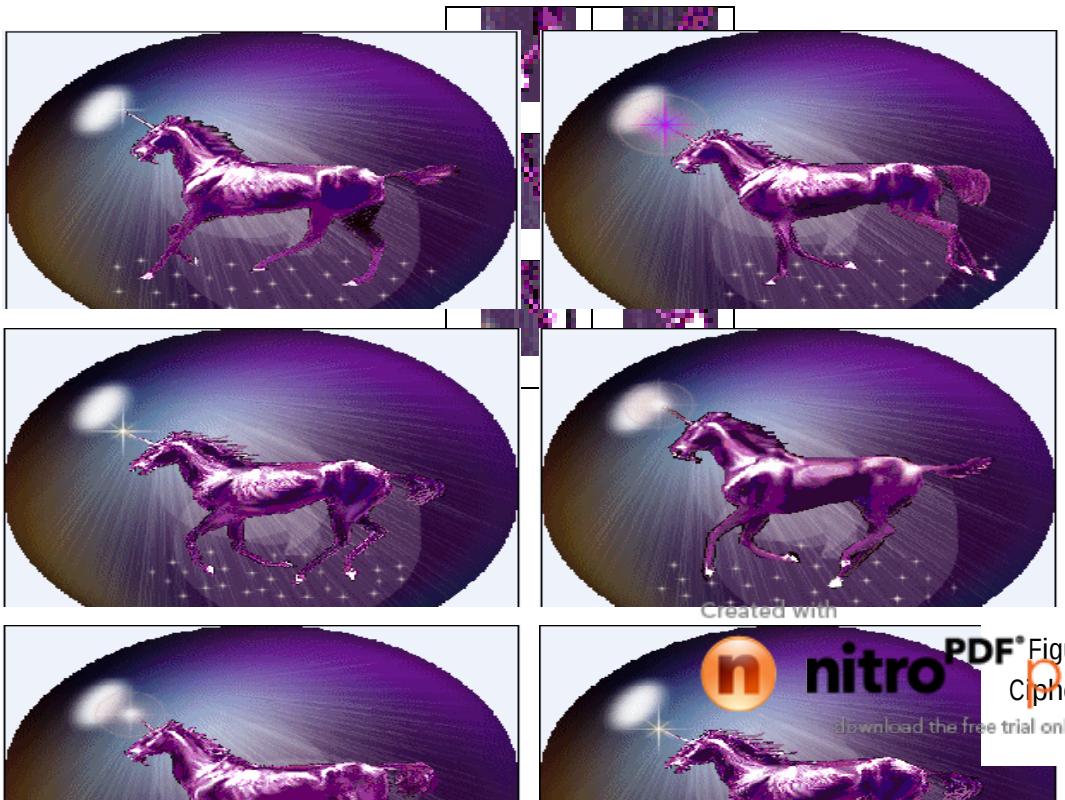


Figure (5): Application of RC6 Cipher to Plain Text Cipher Text Image.

Table (3): Enciphering/Deciphering Speed Test Results

Table

Image size (in pixels)	Colors	Encryption in Sec	Decryption in Sec.
512 x 512	2	0.0011	0.0011
512 x 512	16	0.0091	0.0109
1024 x 1024	2	0.0151	0.0164
1024 x 1024	16	0.0717	0.0833
1024 x 1024	256	0.1619	0.1745
2048 x 2048	2	0.0667	0.0955
2048 x 2048	16	0.2943	0.3803
2048 x 2048	256	0.6323	0.7605

153	101	101	253	249										87	101	75	101
203	153	101	153	249	254	20	75	75	101	75	84	75	75	84	84	84	84
153	204	153	101	153	249	101	75	75	75	84	75	101	75	75	101	87	75
102	153	203	153	101	203	203	204	75	75	84	75	84	75	75	84	87	84
87	101	153	153	101	101	152	52	75	75	75	84	75	84	75	75	101	87
101	87	101	139	153	101	101	204	52	75	75	84	75	75	84	75	84	101
87	101	75	101	203	153	101	153	253	75	75	75	84	75	84	75	75	75
101	87	84	75	101	204	139	101	254	75	75	75	101	75	84	75	75	101
75	104	84	75	84	24	102	153	101	84	31	75	75	84	75	84	75	75
75	101	87	101	75	84	24	153	152	204	153	101	101	101	102	101	47	75
75	84	101	87	75	75	75	204	101	101	153	203	203	153	203	203	101	20
75	75	84	101	84	75	84	75	204	153	101	153	153	101	153	253	203	101
75	75	101	87	101	75	84	75	101	101	203	236	102	203	203	253	253	101
75	75	75	104	84	75	75	101	75	204	101	101	101	253	253	253	253	153
75	75	75	101	87	101	75	75	75	101	153	101	204	253	253	253	253	153
102	75	75	84	101	84	75	75	84	31	101	153	249	204	253	253	253	153
141	84	75	75	84	87	101	75	84	75	20	21	101	101	153	203	249	204
145	135	87	84	101	84	87	75	75	75	84	84	87	101	204	47	153	203
141	84	75	75	75	101	84	101	75	84	75	101	84	101	75	47	75	47
87	101	75	75	75	84	87	84	75	75	84	84	102	87	84	75	75	75

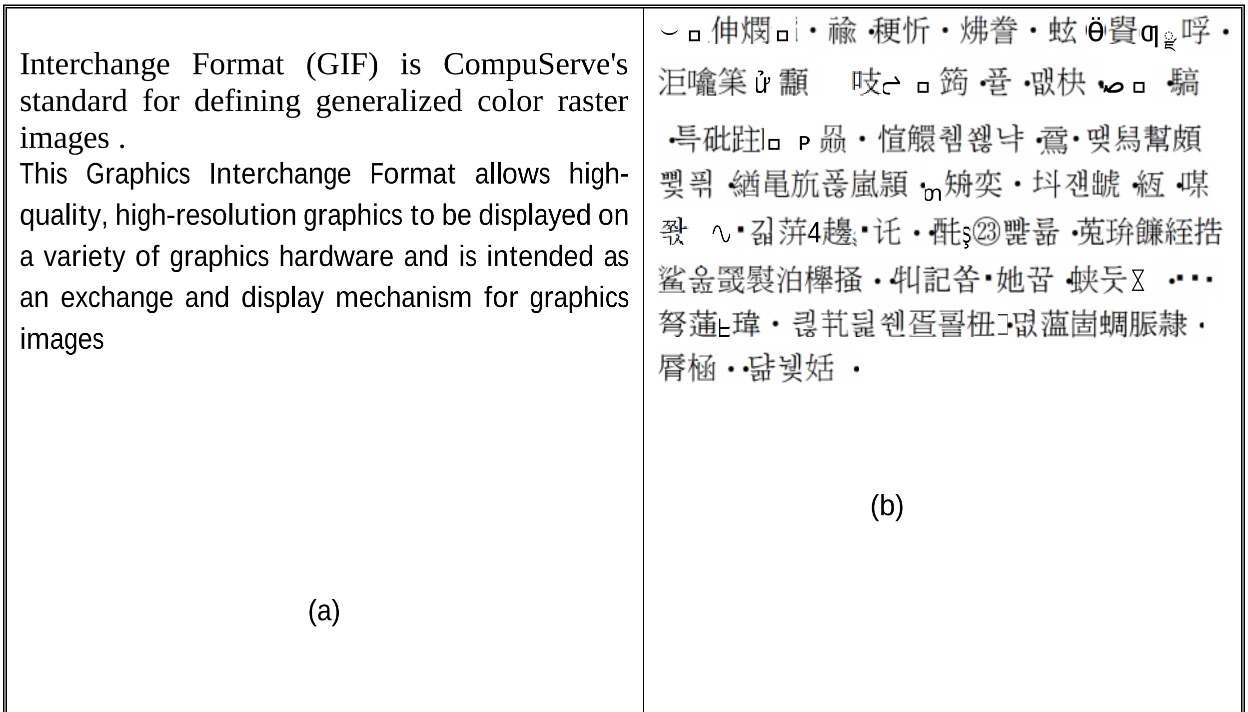


Figure (6):(a) Encrypted Text in Sub Image (b) Decrypted Sub Image

4- Encryption Quality Measurement

Some analysis is to be examined for the measurement of encryption quality and to provide the effect of RC6 block cipher design parameters such as block size, secret key length and number of rounds on the encryption quality of RC6 block cipher for digital images [7].

$$Encryption\,Quality = \frac{\sum_{L=0}^{255} \left| H_L(F') - H_L(F) \right|}{256} \quad ..(1)$$

Table (4) shows RC6 block cipher algorithm at different design parameters. To test the correlation between two vertically

adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in plain image/cipher image, respectively, the procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas [7]:

$$\mathrm{cov}(x,y)=E(x-E(x))(y-E(y)) \quad \text{.....(2)}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{.....(3)}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \quad \text{.....(4)}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \quad \text{.....(5)}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \quad \text{..(6)}$$

Where x and y are GIF image values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used. The correlation coefficients are 0.9919 and 0.0075 respectively for RC6, which are far a part results for diagonal and vertical

Table (4): Different Design Parameters of RC6 Algorithm.

Visual Inspection to Judge the Effectiveness of the Differences	Parameters e	Our Research
W (word size in bits)	16, 32, 64	16 bit
R (No. of rounds)	0, 1, 2.., 255	20
B (Key length)	0, 1, 2.., 255	32
Block size in words	4W	4W
Block size in bites	64,128,256	128
Max block size in bites	256	256
No. of keys derived from key schedule	2r+4	2r+4 = 44

directions were obtained. In this paper, sample form six state were taken to explain the correlation and convolution as shown in the Figure (7).

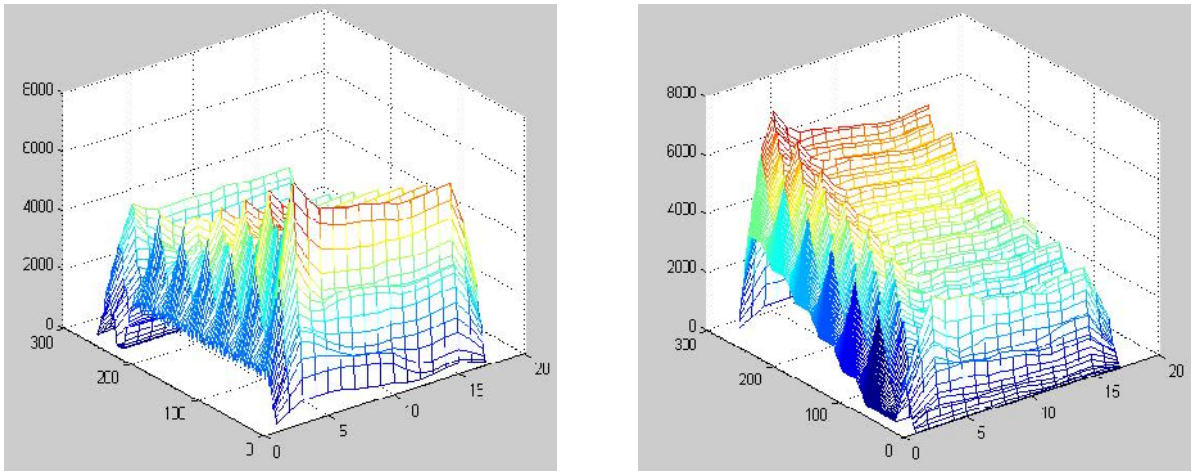


Figure (7): (a) Sample Sub Image Correlation. (b): Sample Sub Image Convolution.

5- Results and Implementation:

This paper introduces a successfully efficient implementation of RC6 block cipher for digital image providing its testing, verification, encryption efficiency analysis, and security evaluation.

A mathematical modeling for encryption efficiency evaluation, that is called encryption quality was proposed, and may be considered to compare the effectiveness of different encryption techniques to digital images instead of visual inspection. The obtained results shows that the RC6 block cipher achieve most better encryption quality for the choices of word size w=4, number of rounds=20, and secret key length b=32. Based on such results, the optimal version of RC6-w/r/b block cipher algorithm that gives maximum encryption quality is estimated to be RC6-32/20/16 From an engineer's perspective, the use of RC6 block cipher algorithm as a candidate for image encryption is very promising for real-time secure image and video communications in military, industrial, as well as commercial applications. Table (5): shows numbers of cycles and speed in RC6 for GIF image.

RC6 no need to reload the round keys every time the user changes the input key.

Table (5): RC6 Implementation for GIF Image.

RC6	GIF at 43.7 MHZ
Key setup	188 cycles 4305 ns
Encryption	21 cycles 480 ns
Decryption	21 cycles 480 ns
Min. Period (ns)	22.881
Max. Frequency (MHz)	43.7
Throughput Including key generation	27 Mbit/sec
Throughput Encryption/Decryption only	266 Mbit/sec

In this work, we satisfy the aim that says the encryption is an effective way to obscure data and hide the sensitive information. The present algorithm allows an individual to hide data inside other data with hopes that the transfer medium will be so obscure that no one would ever think to examine the contents of the file. The algorithm which is described by pseudo-code is presented and it is possible to implement a encryption algorithm to hide a large amount of data into carrier bitmap image. We used three layers of security to secured data by obscuring the context in which it was transferred. With continued research and an improvement in algorithms design, encryption can be taken as a serious way to hide data and the present work appears that it was more efficient than the most familiar algorithm like (S-Tools) [8]. Working against visual and statistical attacks need adaptive algorithm on each step of data embedded.

It was found that the present algorithm was attractive and results reached by this algorithm were efficient in the field of data embedding (encryption). We performed three types of comparison; the first one, was used to compare the present algorithm with S-Tools algorithm through the amount of noise and the amount of size. It appears that the present work was less effective of the noise at the pixels and lager amount of embedded data. The second comparison was made upon the statistical attack; it shows that it was difficult to distinguish between Cover and Stego image when chi square and the difference between neighboring pixels were implemented. The last comparison was found that visual attack results indicate that using non uniform color was extremely powerful when we have large amount of embedded data.

References:

[1] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", International Journal of Computer, Information and Systems Science and Engineering, Winter, 2007.

[2] Hamza A. Ali and Bashar M. Ne'ma2, "Effective Variations on Opened GIF Format Images", IJCSNS International Journal of Computer Science and Network 70 Security, VOL.8 No.5, May 2008.

[3] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images", Journal of Optical Engineering, Vol.45, 2006.

[4] Ralf Steinmetz, Klara Nahrstedt, "Multimedia Systems", Springer, 2004.

[5] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based encryption for digital images and videos", chapter 4 in Multimedia Security Handbook, February 2004.

[6] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Implementation of RC5 Block Cipher Algorithm for Digital Images", Proceeding of The 5th Central European Conference on Cryptography, Brno, The Czech Republic,15-17 June, 2005.

[7] Nawal El-Fishawy and Osama M. Abu Zaid, "Quality of Encryption Measurement of GIF Image Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.

[8] Ronald L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin, "The RC6 Block Cipher", V1.1, August 20, 1998.

[9] Marwa Abd El-Wahed, Saleh Mesbah,and Amin Shoukry, “Efficiency and Security of Some Image Encryption Algorithms”, Proceesings of the World Congress on Engineering, Vol I WCE, London, U.K., July 2-4, 2008.

[10] Yaobin Mao, Guanrong Chen, and Shiguo Lian, “A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps”, Chaos, Solutions and Fractals 21, 2004.