J. of al-anbar university for pure science : Vol.3: No.1 : 2009

ISSN: 1991-8941

A New Steganography Approach depending on Isolation Curve in Digital Images.

Hala Bahjat Abdul Wahab
Computer Sciences Dept.-University of Technology

Received:7/10/2008 Accepted:22/3/2009

Abstract: Curve security involves the process of protecting the shape of the curve from reproduced and as a result, protecting the whole document from being regenerated by any counterfeiting person. The main goal of this paper is combining the curve security concepts with information hiding techniques in order to increase the capabilities of steganography techniques. This paper produced a new data hiding approach for embedded data (text or image …etc) in a digital image by using the gaps locations that generated between curves points, which has isolated parametric curve. Parameterization techniques are greatly affects on curve shape and adds a security features that difficult predict by any counterfeiter. The proposed algorithm will be increased Variable Incremental Growth that rises in parametric Lagrange curve in order to reach robust method for hiding data in digital images. The proposed method was implemented on different sizes of digital images and the results of the proposed approach were been pass and good according to the objective measurements.

Keywords: Graphics, Information hiding, FFT, Parametric Lagrange curves, image processing.

Introduction

Curve security is one of the newest hot spots in security research. The forms produced by graphic systems are much harder to counterfeit, especially when the counterfeiter has no information about how and in which method the design is performed. The shape of the curve is based upon a set of control points that fundamentally describe its properties and its curvature. The algorithms that are used to generate the curves are primarily based on these control points. Thus if the intruder knows the set of control points it may lead to discover the shape of the curves with a trial and error on the method or algorithms that are originally used to produced the curve [1].

Instead of hiding information in all cover the image, a curve selection method is used as positions where the gaps between the points of curve that represent, the secret position to be hidden. The shape of the curve is based upon a set of control points that fundamentally describe its properties and its curvature, these control points represents the secret key to the purposed method and the parameter of time t is the secret. The vibration curve helps to select random position for hiding such that it would be difficult for anyone to guess it. Proposed algorithm employs Lagrange control points of curves as the feature domain, and adopts spread spectrum embedding for robustly watermarking the coordinates of the gaps between the control points[2]. The improvements are presented by: first, generate parametric Lagrange curves according the secret control point and time is the secret key t and increase gapes between points for parametric Lagrange curve second, Extraction of the intensity values of pixels between two control point (take pixels of the gaps ignore all pixels that have no vibration curve out of boundaries of digital image. Third, Applying the Fast Fourier Transform (FFT) for the result intensity values vector. Forth, Embed information using the proposed method that modifies for Least Significant Bit (LSB) by select window size 3*3 of pixel from cover image to hide two characters in nine pixels the center of the window is unused of the real part of FFT for Transform IFFT is apple.

Data hiding in isolation curve.

Lagrange method is a suitable method for interpolation. However, for a big set of control points, the interpolated values tend to draw a vibration curve. Making use of such a vibration in designing a curve that is very difficult for any one to guess its control points. Make use of such a vibration in designing a security curve that is very difficult for any one to guess its control points [3].

Curve security involves the process of protecting the shape of the curve from reproduced and as a result, protecting the whole document from being regenerated by any counterfeiting person.

Variable *Incremental Growth Problem.*

The gaps between the new points in the generate curve appears when the change in the computed value of y=f(x) is greater than the change in the value of (x), and the size of gap varies according to the curve equation that is used to compute the value of y=f(x).

To solve this problem, must be control of the increment value of the new points by making the increment value fixed to all points of the generated curve. Nevertheless, this paper work to increase these gapes in order make the locations for hiding more difficult and embedded the secret massage in the gapes instead the point of the Lagrange curve[4].

Lagrangian polynomial.

The Lagrange polynomial is the simplest way to exhibit the existence of a polynomial for interpolation with unevenly spaced data. The parametric Lagrange interpolating polynomials $L_{N,K}$ has degree N and is one at $x = x_k$ and zero at $x = x_j$ where $j \neq k$.

$$L_{N,K}(t) = \frac{(t-t_0)(t-t_1)\ldots(t-t_{K-1})(t-t_{K+1})\ldots(t-t_N)}{(t_K-t_0)(t_K-t_1)\ldots(t_K-t_{K+1})\ldots(t_K-t_N)} = \frac{\prod_{\substack{j=0 \\ j\neq K}}^{N}(t-t_j)}{\prod_{\substack{j=0 \\ j\neq K}}^{N}(t_K-t_j)} \qquad (1)$$

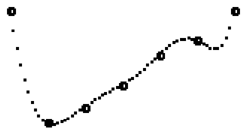
Note that $\prod_{K=1}^{N} K = 1.2.3\ldots N.$ The interpolating polynomial may be written:

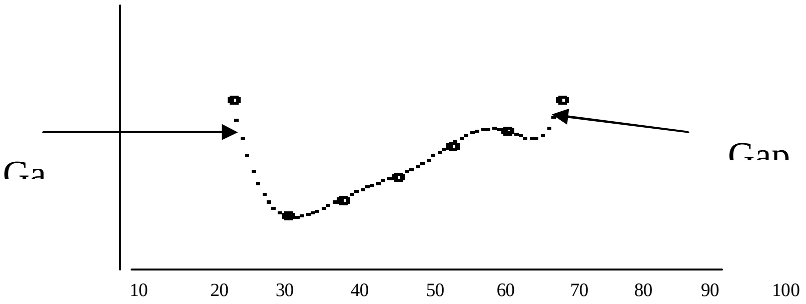
$$P_N(x) = \sum_{K=0}^{N} x_k L_{N,K}(t) = x_0 L_{N,0}(t) + x_1 L_{N,1}(t) + \ldots + x_N L_{N,N}(t) \qquad (2)$$

$$P_N(y) = \sum_{K=0}^{N} y_k L_{N,K}(t) = y_0 L_{N,0}(t) + y_1 L_{N,1}(t) + \ldots + y_N L_{N,N}(t) \qquad (3)$$

It is just a linear combination of the Lagrange interpolation polynomials $L_{N,K}(x)$ With the as y_K the coefficients [5].

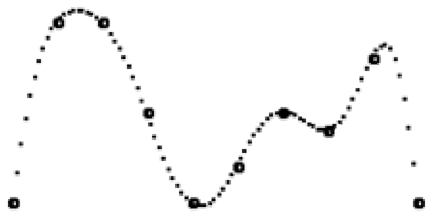
Example1:

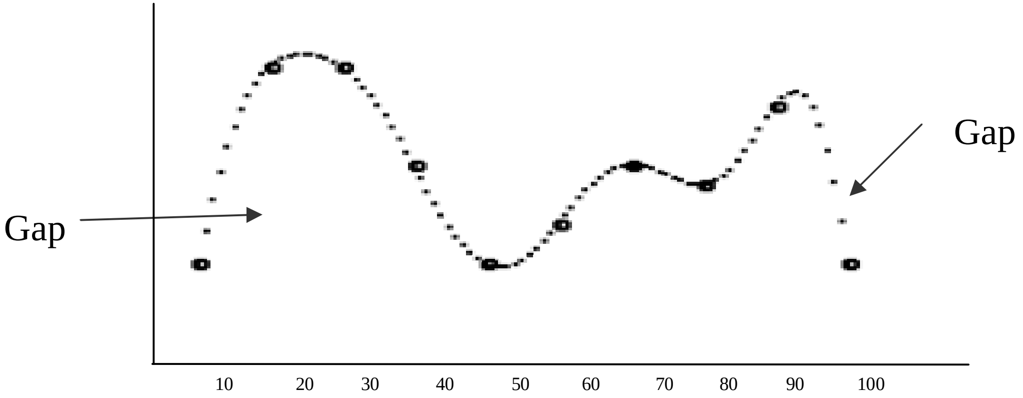
t	X	Y	Interpolated Curve
10	25	100	
20	50	175	
30	75	165	
40	100	150	
50	125	130	
60	150	120	
70	175	100	



Example1 :Lagrange curve with gaps

Example2:

t	*X*	*Y*	*Interpolated Curve*
10	100	300	
20	125	200	
30	150	200	
40	175	250	
50	200	300	
60	225	280	
70	250	250	
80	275	260	
90	300	220	
100	325	300	



example2 Lagrange curve with gaps.

Algorithm 1: Proposed algorithm to generate lagrange curve with increase the gaps between points of curve.

Input: set of control points (x,y), value of parameter t (time) ,let ti=0,…n where Δt=(ti+1-ti)=20

Output: Lagrange curve with big gaps.

Process:-

Step 1:- Set Inc=1

Step 2:- Compute new value of x according the equation:

$$x_{n+1}=x_n+Inc$$

Step3:- Computed new point value (x_{n+1}, y_{n+1}) according to that curve equation (2), for example used the general equation:- $y_{n+1}=y^*(x_{n+1})$ to explain the idea.

Step4:- Compute the difference between the y-values:-

$$E=|y_{n+1}-y_n|$$

Step5:- If (E > 1.5) then

Compute new value with gap the equation:-

gap = E/2

{ compute Gaps coordinates for hiding process}

Y-gap=gap + yn

x-gap=xn

Step 6:- If (E <0.5) then

Compute Inc=Inc*2 and

Repeat from step2 to step4.

Step 7: Compute the point (x_{n+1},y_{n+1}) and Plot (x_{n+1}, yn_{+1}), and go to the step1.

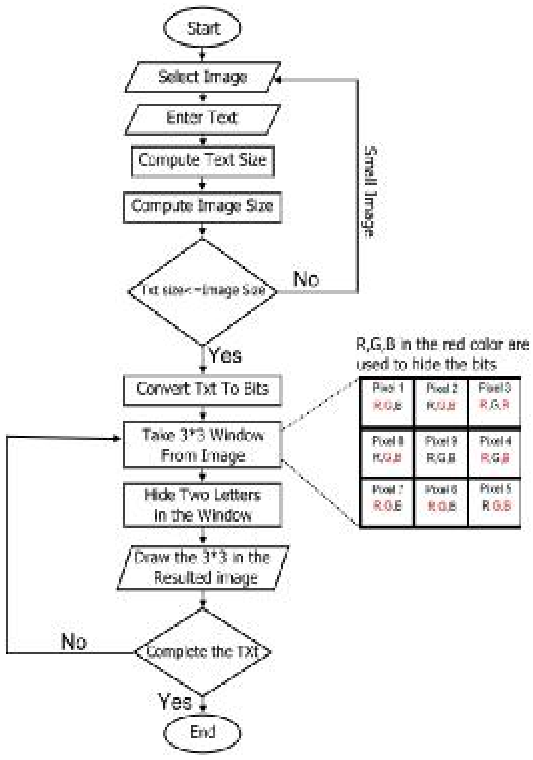
Step 7:-End.

The proposed method for embedded stego-text in image using window method.

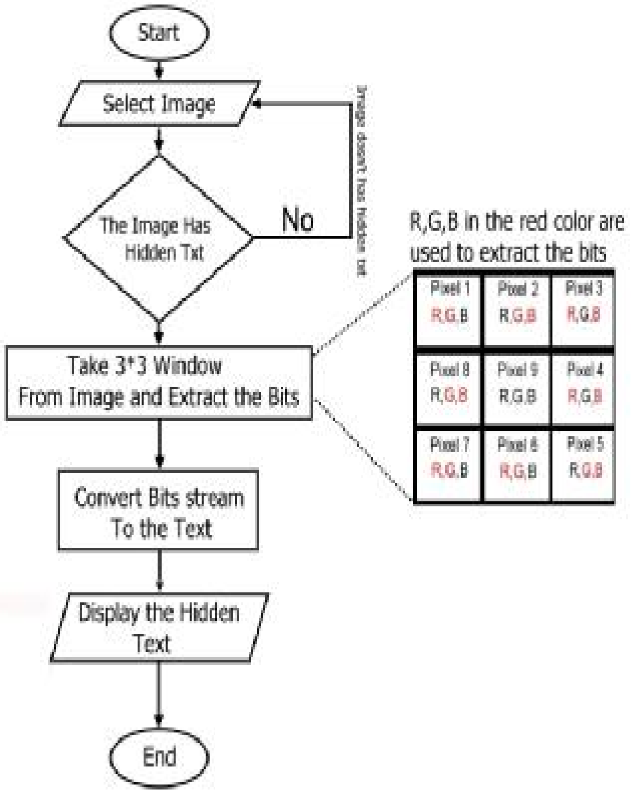
Pixel 1 **R.G. B**	**Pixel 2** **R.G. B**	**Pixel 3** **R.G. B**
Pixel 8 **R.G. B**	**Pixel 9** **R.G. B**	**Pixel 4** **R.G. B**
Pixel 7 **R.G. B**	**Pixel 8** **R.G. B**	**Pixel 8** **R.G. B**

Figure 1: window takes from the cover image.

In this method modify an algorithm which is one of the most important and famous method of steganography that deals with hiding textual information in a typical image files by the Least Significant Bit (LSB) method [6], the proposed method modified the original LSB method , to increased the security of hiding by take window of pixels for example size 3*3 and select the pixel from the window according some schema . Figure 1 show hide two character in nine pixel the center of window is unused. The first character (8 bits) from the message is hidden in (R, D of pixel 1) , (G,B of pixel 2), (R,B of pixel 3), (G, B of pixel 4) and second character in(G,B of pixel 5) , (R,G of pixel6),(R,G of pixel 7)and (R,B of pixel 8) this pattern of color could be changed in any order easily.



(Text Hiding algorithm)



Text Extracting algorithm

The proposed algorithm.

This section depicts the new purposed algorithm for information hiding. The algorithm for hiding is implemented is section(5.1), and the algorithm for extraction is implemented in section (5.2) .

The main algorithm for hiding process:

Input: Cover image, and Secret message bits

Output: Stego-image

Process:

Step1: Select by using the mouse from cover image any number of pixels, which represent the control points.

Step2: Apply parametric Lagrange algorithm to the selected pixels to draw the interplant gap curve-according algorithm 1.

Step3: Extract the pixels that have location in the gapes of curve from the cover image pixels in which the interplant curve not pass by.

Step4: While the extracted image pixels is not empty get the extracted image byte .

Step5: While the hidden message bits, is not empty get a bit using the proposed method of hiding that mentioned in section 4 by using window size 3*3, and assigned it to the first bit of the real part of the DFT of the step4

Step6: Apply the IDFT to the result of step5

Step7: End of while

Step8: End.

The main algorithm for extraction process:

Input: Stego-image and the selected cover image pixels (control points)

Output: Secret message bits

Process:

Step1: Apply parametric Lagrange algorithm to the selected pixels to find the gapes of interplant curve

Step2: Extract the cover image pixels in which the interplant curve not pass by

Step3: While the extracted image pixels is not empty, get the first bit of each byte

Step4: End of while

Step5: End.

Application

Stego-image

Secret massage

Cover image

Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pixel is represented by three bytes, each byte representing the intensity of the three primary colors red, green and blue (RGB), respectively

Objective Fidelity Criteria [7].

The objective fidelity criteria provide equations that can be used to measure the amount of error in the reconstructed images or to measure the amount of error between pure image and stego-image.

Commonly used objective measures are the Root-Mean-Suare error (MSE), Signal-to-Noise Ratio (SNR) and the Peak Signal-to-Noise Ratio (PSNR) .

$$MSE = \frac{1}{H*W}\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}\left(f(x,y) - f'(x,y)^2\right)$$

$$RMSE = \left[\frac{1}{H*W}\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}\left(f(x,y) - f'(x,y)\right)^2\right]^{1/2}$$

$$SNR = \frac{\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}(f(x,y))^2}{\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}\left(f(x,y) - f'(x,y)\right)^2}$$

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right)$$

$$Similarity(A_{ij}, B_{ij}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}a_{ij}b_{ij}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}a_{ij}^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}b_{ij}^2}}$$

Where:
f(x,y) : is the value of the original image at row(y) and column(x),
f ′(x,y) : is the corresponding values of the stego- image,
H , W : the height of the image and the width of the image respectively,
Aij ,Bij : two images matrices size (N×N).

File name	File size	RMSE	SNR	PSNR	SIM
Imge0 Stego_imge0	23KB	0.0199	5.5176	82.1740	0.9464
Imge1 Stego_imge1	7KB	0.0241	6.516	72.217	1
Imge2 Stego_imge2	10KB	0.0135	20.4964	85.5506	0.9974
Imge3 Stego_imge3	13KB	0.0521	5.213	62.301	1
Imge4 Stego_imge4	19KB	0.0192	10.1796	82.4677	0.9988

From the results of the measures obtained the following results:-

1- The small results of RMSE means no conceal information in the image after hiding process.

2- The results of SNR and PSNR means give the same results that no information loss in the stego-image.

3-The similarity measure shows the amount of correlation between the original image and stego- image and the result from this test is acceptable.

Conclusions

1. Different selection to different number and positions of image pixels by mouse gives the interplant curve different shapes. Hence, adds a security feature that difficult to predict by any counterfeiter.
2. The use of the gapes in Lagrange curve as a method for embed process, gives good results according the results of objective measures.
3. control points play an important role when it is used as a secret key (primary key).
4. The DFT is one of the frequency domain methods, which is more secure then the time domain in (LSB) methods.
5. This approach could be implemented to any image file type.

References

[1] Firas Husham Al-Mukhtar(2003). ”Parallel Generation of Non Linear Curves with Computer Aided Application”, PhD. Thesis, Computer & Informatics Information Institute for Postgraduate Studies .

[2] Neil F. Johnson, Sushil Jajodia, “Steganalysis of Images Created Using Current Steganography Software,” Center for Secure Information System, Second International Workshop, Springer Verlag, April 1998.

[3] Stefan Katzenbeisser and Fabien A.P. Petitcolas,” Information Hiding Techniques for Steganography and Digital Watermarking,” Artech House, INC, London, June 2000.

[4] Anthony Ralston and Philip rabinowitz, (1978). ” First Course in Numerical Analysis”, second edition, McGraw-hill Inc.

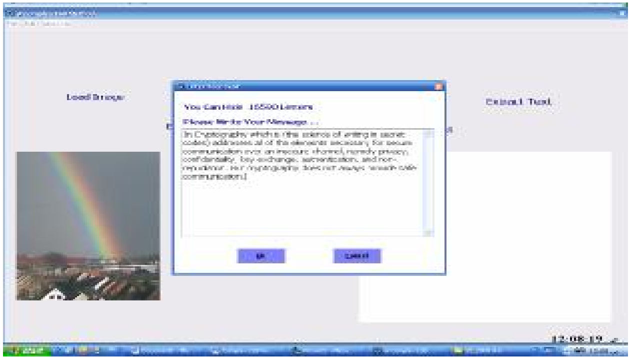
[5] Goldman Ron, (2002). ”Lagrange Interpolation and Neville’s Algorithm”, Department of computer Science ,Rice University.

[6] N. F. Jonson, Z. Duric, and S. Jajodia, "Information Hiding: Steganography and watermarking_Attacks and Countterersures", Kluwer Academic Publishers, 2001.

[7] Scotte E. U., (1998). ”Computer Vision and Image Processing :Practical Approach Using CVIp Tools”, Prentice-Hall ,Inc.

Appendix:

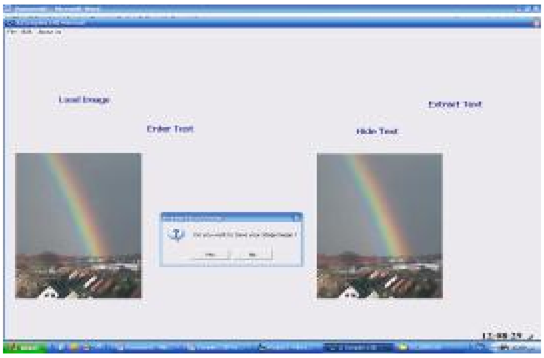
Example 1:



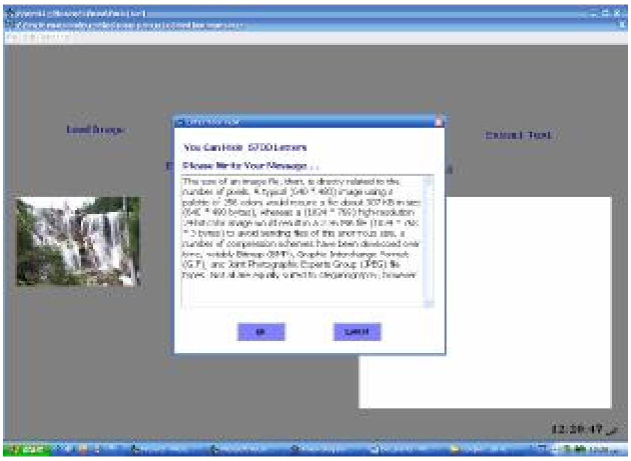
You Can Hide 16500 Letters

Please Write Your Message ...

In Cryptography which is (the science of writing in secret codes) addresses all of the elements necessary for secure communication over an insecure channel, namely privacy, confidentiality, key-exchange, authentication, and non-repudiation. But cryptography does not always provide safe communication.]



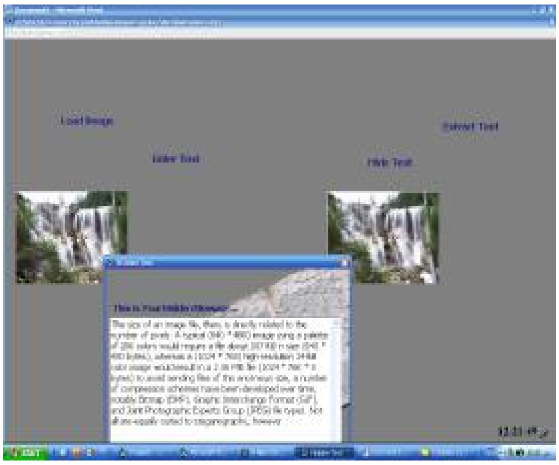
Example2:



You Can Hide 5700 Letters

Please Write Your Message ...

The size of an image file, then, is directly related to the number of pixels. A typical (640 * 480) image using a palette of 256 colors would require a file about 307 KB in size (640 * 480 bytes), whereas a (1024 * 768) high-resolution 24-bit color image would result in a 2.36 MB file (1024 * 768 * 3 bytes) to avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to steganography, however



This is Your Hidden Message ...

The size of an image file, then, is directly related to the number of pixels. A typical (640 * 480) image using a palette of 256 colors would require a file about 307 KB in size (640 * 480 bytes), whereas a (1024 * 768) high-resolution 24-bit color image would result in a 2.36 MB file (1024 * 768 * 3 bytes) to avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to steganography, however

طريقة جديدة لإخفاء البيانات في الصور الرقمية بالاعتماد على الفجوات الناتجة من تذبذب منحنى

هاله بهجت عبد الوهاب
E.mail: hala_bahjat@yahoo.com

الخلاصة:

أمنية المنحنى تساهم في عملية حماية شكل المنحنى من اعادة توليده وكنتيجه لهذا يتم حماية المستند من محاولة توليده عن طريق المهاجم . الهدف الرئيسي لهذا البحث هو دمج بين مفاهيم سرية المنحنى وتقنيات الاخفاءوذلك لزيادة امكانيات اخفاء المعلومات وتقنياته . البحث يقدم طريقة جديدة لطمر المعلومات (نص او صوره ... الخ) في صوره رقمية من خلال استخدام مواقع الفجوات المتولده بين نقاط منحنى المتذبذب كمواقع لاخفاء المعلومات داخل الصوره الرقمية . تقنيات البارامترات تؤثر بشكل واسع وكبير على شكل المنحنى وتضيف خصائص تصعب تخمينها من قبل المهاجم. الخوارزمية المقترحة تعمل على زيادة حجم الفجوات التي تظهر في منحنى لاكرانج لغرض الوصول الى طريقة قوية في اخفاء المعلومات في الصور الرقمية , الطريقة المقترحة استخدمت صور رقمية باحجام مختلفه وكانت النتائج جيده ومشجعه حسب المقاييس والفحوصات المعتمدة.