Using Generated Digital Images in Image Cryptography

Dr. Hala Bahjat Abdual Wahab
University of Technology
Baghdad/Iraq
Hala_bahjat@yahoo.com

Dr.Yossra Hussain Ali
University of Technology
Baghdad/Iraq
Yossra_h_a@yahoo.com

Dr.Alia Karim Abdul Hassan
University of Technology
Baghdad/Iraq
hassanalia2000@yahoo.com

ABSTRACT

The end product of a computer graphics process is usually an image or sequence of images. The image may be displayed on a variety of devices, depending on the application. In this paper we perposed algorithms to generated 2D-image as bitmap image and use this image as a key to encrypt the image (bitmap or JEPG image) (i.e. cipher image by image). Moreover, we can clip the Bezier curve from the generated image that have randomness property to encrypt the images according to the know randomness tests .

استخدام الصور الرقميه المولده في التشفير الصوري

الملخص

في السنوات الاخيرة الماضية أمنية الحاسوب أخذ بأعادة تطوير نفسها حيث أن ظهور التكنولوجيا الحديثة و التطبيقات الجديدة جلبت تهديدات جديدة خاصة مع نمو المتزايد في مجال الاتصالات ونقل البيانات . هذا الذي جعل الحاجة الى التشفير وأمنية البيانات من المتطلبات الاساسية في كافة مجالات الاتصالات ونقل وحماية البيانات .

واحد من أسخن النقاط في مجال البحوث الامنية هو أمنية المنحني، حيث ان الاشكال التي تنتج من أنظمة الرسم بالحاسبة تكون اكثر صعوبة امام المقلد خاصة عندما لا يكون لديه اي معلومة حول بيانات وخوارزمية الطريقة التي استخدمت .

أن الهدف الاساسي في هذا البحث هو دمج بين أمنية المنحني و خوارزميات التشفير من أجل زيادة أمكانيات التشفير الصوري. حيث ان الضعف في مفتاح التشفير المولد بواسطة الصور الاعتيادية واضح بسبب التقارب القيم اللونية للصورة هذا الذي قادنا في هذا البحث الى تقديم طريقة جديدة لتوليد مفتاح التشفير صوري بالاعتماد على توليد نماذج رياضية ثنائية وثلاثية الابعاد ومن ثم أستقطاع مفتاح التشفيربالأعتماد على بيانات وخوارزمية توليد المنحني . وقد فحص النتائج بأعتمادعلى المقاييس الشائعة في هذا المجال والتي أعطت نتائج مشجعه .

Keywords: Applied Cryptography, Graphics, Image Generation, Random Number Generator, and image cryptography

1. Introduction

Counterfeiting is a growing threat in recent years, especially with the ever-increasing growth of data communication, the need for security and privacy has become a necessity. Cryptography and data security are an essential requirement for communication privacy. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot read by anyone except the intended recipient [Den83].

Computer graphics is a topic of rapidly growing importance in the computer field. It always has been one of the most visually spectacular branches of computer technology, producing images whose appearance and motion make them quite unlike any other from of computer output [New81]. The shape of the curve is basically based upon a set of control points that fundamentally describe its properties and its curvature. The algorithms that 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[Jea00].

2. *Generating 2D Image using parametric Lagrange curve and Rolling Circle Movement*

In this section, a new method proposed to generate 2D image (digital image) using moving rolling circle around the parametric Lagrange curve that as a tool for generating the digital image.

The image that we want to generate must have the following properties:-

1- The image must not be regular, i.e. does not contain identifiable objects or pattern and cannot described to any one by any body.

2- It is difficult or infeasible reproduction of the image by counterfeiter unless one knows all the algorithms used to generate the image are known and all the parameter values.

3- The image must have randomness color property (pixels values) that makes the image useful in security field.

The process to generate 2-dim image consist of the following stages:

<u>Stage One</u>

Initialize 2D-mesh of control points that used to generate a curve according to algorithm (1).

Initializing 2D-mesh which achieved by selecting a set of control points according to a determined increment value between control points. Increment value for x-coordinate or y- coordinate or both, and the increment value may be a fixed value or a variable value.

All these choices studied and we concluded that the increment value plays an important role in the generated image, since any change in increment value generates new mesh of control points and will lead to a new image with the new features. This property gives security condition to the image, because the counterfeiter will face a difficult process to guess the start control points and the increment value of the x-coordinate or of the y-coordinate or both.

Figure (1) shows an example of a 2D- mesh of the control points with equal increment to x-, y- coordinates.

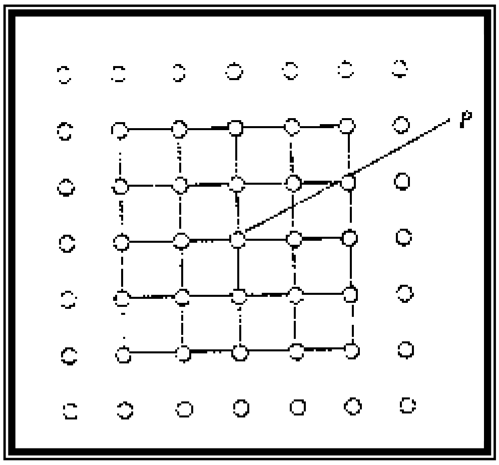


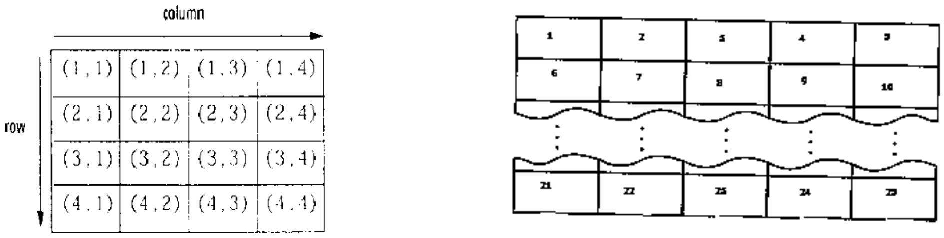
Figure (1): Mesh of control points (p).

Stage Two

In this stage, we are moving the generated curve according to algorithm (2) through the 2D-mesh that initialized in stage one.

This process is achieved by marking the control points on the mesh by a simple way like counting the control points for example 1, 2, 3…and so on, and entering number of control points of 2D-mesh to a simple pseudo-random generator.

The pseudo-random generator gives each time a set of numbers that is represented as addresses of the control points in the 2D-mesh in a random way using to generate (interpolate) the curve. Figure (2) shows two examples for marking 2D-mesh;where figure (2-a) shows an example of marking a mesh of size (4×4) of control points and Figure (2-b) shows an example of marking a mesh of size (5×5).



(1,1)	(1,2)	(1,3)	(1,4)
(2,1)	(2,2)	(2,3)	(2,4)
(3,1)	(3,2)	(3,3)	(3,4)
(4,1)	(4,2)	(4,3)	(4,4)

(a) Mesh size (4×4)

1	2	3	4	5
6	7	8	9	10
⋮	⋮	⋮	⋮	⋮
21	22	23	24	25

(b) Mesh size (5×5)

Figure (2): Examples for marking meshes of control points.

Stage Three

In this stage, after executing stage two, determining the generated image boundaries performed. A large number of recursive pixels will be obtain and spread on the screen of the computer by an isolation way according to the isolation movement of the generated curve.

Determining the image boundaries is achieved by delete all the pixels out of the fixed boundaries of the image. The size of the image (boundaries) is suitable to keep secret between the sender and the receiver only. In the following, we describe the proposed complete algorithms for generating 2D image using parametric Lagrange curve with a moving rolling circle around it.

Algorithm (1): Generate curve using parametric Lagrange method.

```
Input:   Given set of N+1 data pairs($x_i$,$y_i$), i=0…N, and given
          values of parameter $t_i$=0,…,N, where Δt=($t_{i+1}$-$t_i$)=10.
Output: Generate parametric Lagrange curve.
Process:
Step1:   Set res=0, k=1, step=1, N=10, h=1
Step2:   Temp (h) =t (k)
Step3:   While (k <> N) do
          While (Temp (h) >=t (k)) and (Temp (h) <=t (N)) do
Step4:    res=0
          For i=1 to N
          P=1
          For j= 0 to N
          If i <> j then p =p *(Temp (h) - t (j))/ (t (i)-t (j))
          Next j
Step5:    res=res+ (p*x (i)), Next i
Step6:    New_x (h) =res,
          res =0, h=h+1,
          Temp (h) =Temp (h-1) +step
Step7:   loop,
         k=k+1, loop,
 Step8:  Goto from step 1 to 4.
         res =re s+ (P*y (i))
         next i
Step9:   New_y(h)=res, res=0,h=h+1,
         Temp(h)=Temp(h-1)+step
         Loop, k=k+1, loop
Step10: For i= 1 to h
          Plot (New-x, New-y)
          Next i
Step11:  End.
```

Algorithm (2): Moving the rolling circle around Lagrange curve.

```
Input:  Take pairs of data (New-$x_i$, New-$y_i$), i=0,..,h-1, that computes  in
         algorithm (1) to represent the x –coordinate (x-c) and y-
         coordinate (y-c) to center of circle, and input the radius circle.
Output:  Moving rolling circle around parametric Lagrange curve that
           generate in algorithm (1).
 Process:
Step1: Set radius=15
```

```
Step2: For i= 0 to h-1
            Set x-c= New-x, y-c=New-y
             For index=0 to 360
                X=radius*cos (index) +x-c
                Y=radius*sin (index) +y-c
Step3: Plot (X, Y)
Step4: Next index, Next i
Step5: End.
```

Algorithm (3): Generate 2D Image

Input: Input a first control point, increment value (Inc), size of mesh control points (N×N) and size of the image that want to generate.

Output: Generate 2D digital image.

Process:

```
Step1: Initialize the mesh of control points according to the start control
       points; increment the value and the size of the mesh.
Step2: Mark the control points of the mesh.
Step3: Enter the number of marks to simple pseudo-random generator.
Step4: Take the sequence of output from the generator to represent the
       addresses of the set of control points in the mesh.
Step5: Perform the Algorithms (1) and (2) to draw the parametric Lagrange
       curve with rolling circle.
Step6: Repeat step4 with new sequence of numbers and step 5 until obtaining
       the recursive pixels that covers the image size that need to generate.

Step7: Clip the image according to the size the user entered.
Step8: Obtain the 2D generated image.
Step9: End.
```

<u>Example:</u>

In the following example a 2D-image is generated using a mesh size of (25×25) with the same increment value of x-,y-coordinates equal to (10), and using a radius for the rolling circle equal to (15), and the image size that need to be generated is equal to (256×256) pixels.

Figure (3) shows the oscillation curve movement by random way through the 2D-mesh is due to the movement of the curve path out of the mesh boundary.

Figure (4) shows the final stage of generating the 2D-image by clipping the image size to (256×256) pixels.

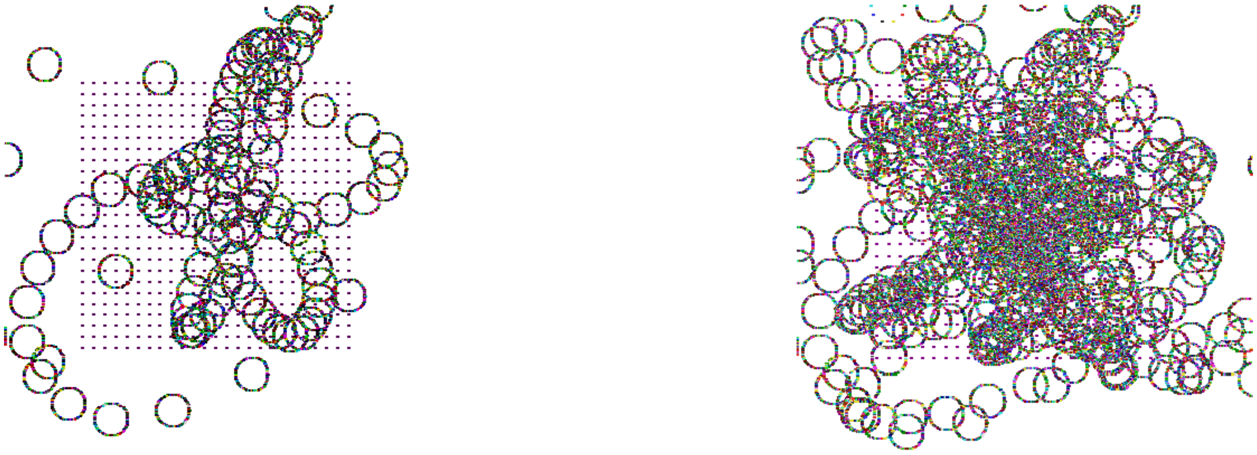


Figure (3): Example shown the oscillation moving curve through 2D-mesh.

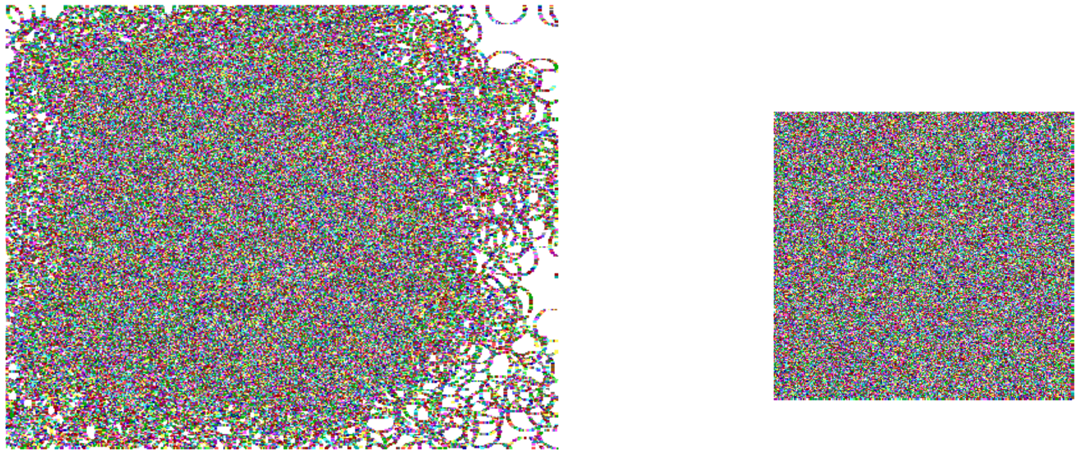


Figure (4): Example to clip image size 256×256 pixels.

3. *Image Cryptography*

The cornerstone of all privacy mechanisms is encryption, which may be viewed as the process of transforming image documents, using a secret key, into ciphered image document. Only individuals who know the key can decrypt the ciphered image document to recreate the original image documents [Dal04].

Cryptography can provide practical solution to the protection of stored image document, in terms of both the nondisclosure of confidential images and the detection of unauthorized modification of image documents.

Image cryptography hasn’t been widely studied as normal cryptography or visual cryptography. It was used by Zenon et al. [Zen97], to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access.

Image cryptography is one of the fields based on both image processing and cryptography, which concerned with ways to encrypt pictures, i.e. information which can be perceived directly by Human Visual System (HVS) [Ste92]. In figure (5) shown the basic concept of image cryptography.

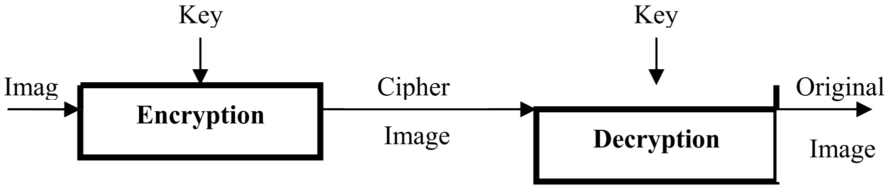


Figure (5) : image cryptography concept.

3.1 Residual Intelligibility and Regularity of Digital image

When ciphering systems are constructed, there must be some techniques to show the amount of ***residual intelligibility*** in ciphered images, and the quality of the reconstructed images. The Ciphered Image must be considered nearly as white noise (chaotic) with low ***residual intelligibility*** and low quality, on other side the reconstructed (deciphered) image, must give high intelligibility and high quality with high level of regularity[Reg01].

Algorithm(4): Image cryptography using generated image.

The following illustrates the proposed algorithm to cipher image by generating image and ciphered image by clipped curve from generated image.

Input: clipped curve randomness pixels or part (slide) from generated image and save slide as bitmap image (true color) and save the clipped curve pixels in file (clip. dat). And input the image (JEPG or Bitmap) that want to ciphered **.**

Output: Obtain to the ciphered image.

Process:

```
Step1: open the generated image and perform the following process to
       separate the color pixels(RGB) to red ,green and blue and save
       colors(R,G,B) in one-dimension array (pic1)and repeat the process
       on the image that want to be ciphered and save in array (pic2)
        For i = 0 to height
        For j = 0 to width
        pixel = Picture1.Point(i, j)
         r = pixel& Mod 256
     pic1(k1) = r
      k1 = k1 + 1
      g = ((pixel& and &HFF00FF00) / 256&) Mod 256& pic1(k1)
      b = (pixel& and &HFF0000) / 65536
      k1 = k1 + 1
      pic1 (k1) = b
     k1 = k1 + 1
      Next j
```

```
        Next i
Step2: If (the user want to cipher image by generated bitmap image) then  go
        to 3
        If (the user want to cipher image by clipped curve) then
        go to  5
Step3: (encrypt image by image)
        Perform XOR operation directly on the two images pic1 and pic2 and
        save the result in third picture (pic3) as follow:
        Set   k3 = 0
        For i = o to k1 - 1
        pic3 (k3) = pic1 (i) XOR pic2 (i)
        k3 = k3 + 1
        Next i
Step4: Separate the three colors (R,G, B) and save the  three one-
        dimension arrays red, green and blue and then use the function (RGB)
        to obtain the true color pixels.  This process performs as follow:
        Set i = 0, k1 = 0, k2 = 0, k2 = k3 / 3
        Do While i < k2
        red (i) = pic3(k1)
        k1 = k1 + 1
        green (i) = pic3(k1)
        k1 = k1 + 1
        blue (i) = pic3(k1)
        k1 = k1 + 1
        i = i + 1
        loop
        k1 = 0
        For i = 0 to x1 - 1
        For j = 0 to y1 - 1
        a(i, j) = RGB(red(k1), green(k1), blue(k1))
        Picture3.PSet (i, j), a(i, j)
        k1 = k1 + 1
        Next j
        Next i
Step5:  (encrypt image by Bezier curve)
         Open the file (clip. dat) that save the curve pixels then repeat the
         steps 3 and 4 using the file instead of (pic1).
Step6:  end.
```

In the following figure (6) shown the block diagrams for proposed algorithm.

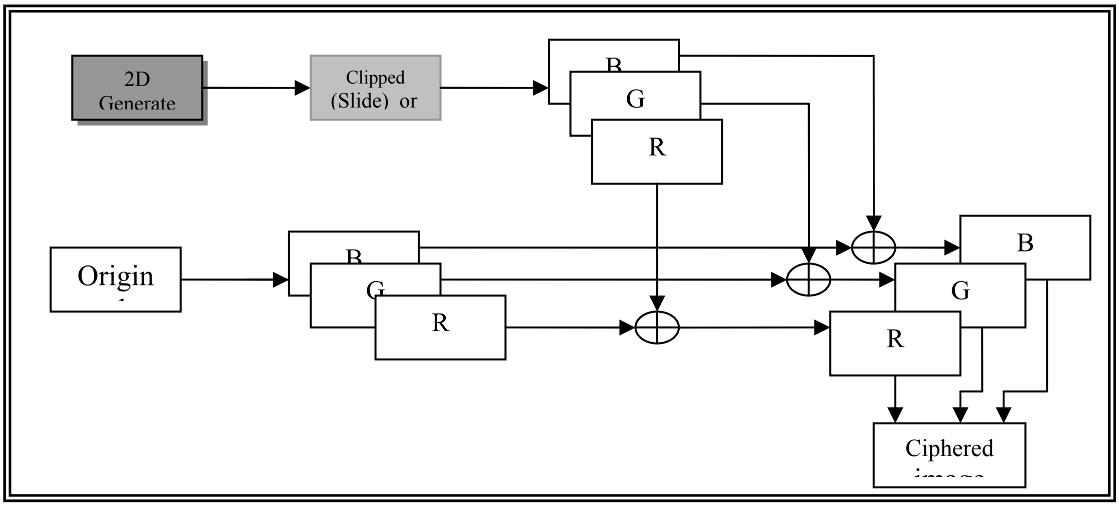


Figure (6): Block diagrams for proposed algorithm (4).

Examples

The following examples of images show the results of implementing the pervious algorithm for encryption images on different image types (Bitmap and JEPG) using bitmap generated image and using clipped Bezier curve pixels.

Original Image

(JEPG image)

Key (Bitmap-Generated Image)

Ciphered Image

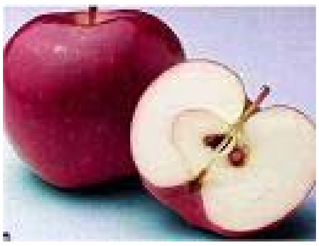
(JEPG image)

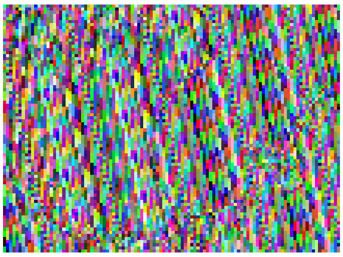
Size 128×100 KB

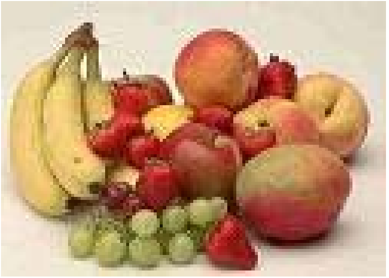
Size 126×90 KB

Original Image
(JEPG Image)

Using Bezier Curve pixels as a key to
Ciphered Image. (JEPG Image)







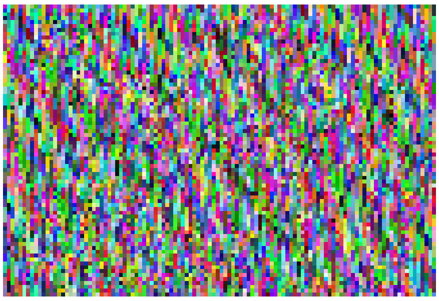


Table (1): shown the test results for ciphering images (JEPG) by 2D-generated Bitmap Image.

Image	*MSE*			*PSNR*			*SNR*			*Similarity*		
Name	***R***	***G***	***B***	***R***	***G***	***B***	***R***	***G***	***B***	***R***	***G***	***B***
Apple	11858.01	13124.42	3779.21	1.81	1.68	1	4.55	3.11	2.30	0.22	0.28	0.12
Fruit	12008.60	11074.46	3210.77	1.79	1.90	2	5.23	4.13	3.73	0.18	0.12	0

Table (2): shown the test results for ciphering images (JEPG) by clipped curve from generated Bitmap Image.

Image	*MSE*			*PSNR*			*SNR*			*Similarity*		
Name	***R***	***G***	***B***	***R***	***G***	***B***	***R***	***G***	***B***	***R***	***G***	***B***
Apple	12102.63	144498.25	4193.79	1.78	1.56	1	4.46	2.66	1.81	0.20	0.13	0.21
Fruit	12636.29	11193.87	3226.05	1.73	1.88	2	5.00	4.11	3.70	0.18	0.13	0.01

4. Conclusions

From the results of the measures that were used to test the ciphered images, we can obtain the following:-

1- The large results of MSE and RMSE means the proposed key is succeeded to conceal pure image information (i.e. there are large errors in ciphered image caused by the use of the proposed key.).

2- The small results of SNR and PSNR means the proposed key caused large noise (i.e. small, a result implies better image concealment of original image.).

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

4- The clipped curve generated from 2D generated mathematical models (digital images) gives reasonable results in order to be used as a key in image cryptography according to the measure tests that used in the field

5. *References*

[Den83] Denning D. E., (1983). ***"Cryptography and Data Security"***, Addison-Wesley Publishing Company, Inc.

[New81] Newman W.M., Sproull R.F., (1981). ***"Principles of Interactive Computer Graphics"***, Mc Graw-Hill Book Company London.

[Sch99] Schaefer E. D., (1999) . "**An introduction to Gryptography",** Santa Clara University.

[Dal04]] Dallwitz M. J. , (2004). "***An Introduction to Computer Images***", http:// delta-intkey.com.

[Jea00] Jean Gallier, (2000). "**Curves and Surfaces in Geometric Modeling",** Morgan Kaufman Publishers.

[Lew69] Lewis, P., Goodman, A., and Miller, J. ,(1969). "**A Pseudo-Random Number Generator for the System/360."**IBM systems Journal, No.2.

[Zen97] Zenon H., VoloshynovskiyS., Rytsar Y., (1997). "***Cryptography and Steganography of Video Information in Modern Communication***", in Third TELSIKS'97, Yugoslavia, pp. 115-125.

[Ste00] Stefan Katzenbeisser, Fabien A. P. P, (2000). " ***Information Hiding Techniques for Steganography and Digital Watermarking***", Artech House, Inc.