# Modify Symmetric Block Cipher Algorithm Using Generated Digital 3D Fractal Image

**Hala B. Abdul Wahab[1] , Sura A. Sarab[2]***

[1]Department of Computer Science, University of Technology, [2] Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.

## Abstract

The principal goal guiding any designed encryption algorithm must be security against unauthorized attackers. Within the last decade, there has been a vast increase in the communication of digital computer data in both the private and public sectors. Much of this information has a significant value; therefore it does require the protection by design strength algorithm to cipher it. This algorithm defines the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. The Performance and security level is the main characteristics that differentiate one encryption algorithm from another. In this paper suggested a new technique to enhance the performance of the Data Encryption Standard (DES) algorithm by generate the key of this algorithm from random bitmaps images depending on the increasing of the randomness of the pixel colour, which lead to generate a (clipped) key has a very high randomness according to the know randomness tests and adds a new level of protection strength and more robustness against breaking methods.

**Keyword:** encryption algorithms, DES algorithm, key generation, cryptographic key, fractal image generation, diamond square algorithm.

# تعديل خوارزمية التشفير الكتلي ذات المفتاح الواحد باستخدام توليد صورة رقمية كسرية ثلاثية الابعاد

**هالة بهجت عبد الوهاب[1]، سرى عبد سراب[2]**

[1]قسم علوم الحاسبات، الجامعة التكنلوجية، [2]قسم علوم الحاسبات، كلية العلوم، جامعة بغداد، بغداد، العراق.

## الخلاصة:

الهدف الرئيسي الذي يدل على اي خوارزمية تشفير مصممة يجب ان يكون الأمان ضد المهاجمين غير المخولين. خلال العقود الاخيرة، هناك زياده سريعة في الاتصال عن طريق بيانات الحاسبة الرقمية في كلا القطاعين السري والعلني، وبما ان أكثر هذه المعلومات لها قيمة مهمة لهذا فهي تحتاج الى الحماية من خلال تصميم خوارزمية قوية لتشفيرها، هذه الخوارزمية تعرف الخطوات الرياضية المطلوبة لتحويل البيانات الى شكل مشفرسري وكذلك أرجاع الشكل المشفر الى الشكل الاصلي. أن الانجازية ومستوى الامان هي الخواص الرئيسية التي تميز احدى خوارزميات التشفير عن الاخرى، وفي هذا البحث اقترحت تقنية جديدة لتحسين أنجازية خوارزمية تشفير البيانات القياسية عن طريق توليد مفتاح هذه الخوارزمية من الصور النقطية العشوائية بالاعتماد على زيادة عشوائية لون النقطة، وبالتالي توليد مفتاح ( مستقطع ) له عشوائية عالية جدا وفقا الى الفحوصات العشوائية المعروفة وأضافة مستوى جديد لحماية اقوى وأكثر شدة ضد طرق الكسر.

*Email: Suraaljanaby84@yahoo.com

## 1. Introduction

Encryption technology allows people using electronic networks to ensure that the message they send remain private (secure) from hackers, industrial espionage, government wiretap abuses and spies [1]. Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.

Although the ultimate goal of cryptography, and the mechanisms that make it up, is to make obtaining the information too work-intensive to be worth it to the attacker.

Different types of cryptography have been used throughout civilization, but today it is deeply rooted in every part of our communication and computing world. Automated information systems and cryptography play a huge role in the effectiveness of militaries, functionality of governments, and economics of private businesses. As our dependency upon technology increases, so does our dependency upon cryptography, because secrets will always need to be kept. [2]

The great developments in cryptography tend to use keys (in encryption and decryption operations) to increase the complexity of attack operations. For security purposes, the key length should be as big as the size of the plaintext message.

Get such a key and merging it is a real problem in cryptography. This problem may be solved by using random number generator but cryptographic systems need a cryptographically strong random numbers that cannot be break (guessed) by the attacker. Random numbers are typically used to generate a session keys, and their quality is critical for quality of the resulting cryptosystems. [3]

Historically, encryption systems have two types: the first type is private key or symmetric systems that use the same key for both encryption and decryption, a symmetric key is a string of random bits; simply the number of random bits in it measures the keys variability and strength. Cryptographers recommend that, to be reasonably secure, the keys should be at least 90 bits long. The world standard is 128 bits which that is a convenient size for a computers. There is no technical reason to use shorter keys. [4]

The second type of encryption, is known as the public key or asymmetric systems, which uses a separate keys for encryption and decryption: private key and the public key, the properties of cryptographic key are:

- Keys must be unguessable, in the sense that any effort that would enable the key to be discovered must be deemed outside the abilities of the presumed attacker. This implies that a key must be computationally infeasible to exhaustively search (or therwise to prevent the attacker from confirming a guess at the key, though this is typically much harder). In addition , the key must remain computationally infeasible to find in light of all the information the attacker is able to gather about it.
- Keys must be reproducible by intended parties when needed to perform cryptographic operations. Since each cryptographic encoding has a corresponding decoding action, and since at least one of these two (and often both) requires possession of the secret key, typically the key will need to be reproduced spatially or temporally. [4]

For example, a key may need to exist at two different computers simultaneously (a spatial reproduction) if they are interacting in a cryptographic communication protocol. A key may need to exist in the same computer at different times (a temporal reproduction), but not in the intervening period, if the key is used to encrypt and decrypt files on the computer. [4]

In a block cipher algorithm, the plaintext is divided into blocks of bits, usually of a fixed size, and operates on each block independently to produce a sequence of cipher block. Block ciphers tend to simultaneously encrypt groups of characters of a plaintext message using a fixed encryption transformation [5]. These groups of characters are then put through substitution, transposition, and other mathematical functions. the functions map bit strings of a fixed length divided to bit strings of the same length, which is called block size. The cryptographic key controls the functioning of the block cipher and thus, by extension, controls the modes, because the specification of the block cipher itself is typically made available to the public.

The algorithm dictates all the possible functions available to be used on the message, and the key that will determine what order these functions will take place. [2]

Input blocks to the block cipher algorithm must be the same as the size of the output blocks. Block cipher are simple substation cipher and must have large alphabet to fail frequency analysis. One example of block cipher that used in this paper is Data Encryption Standard (DES). A secret cryptographic key (a symmetric key block cipher algorithm) must be entered into the device implementing the block cipher as shown in Figure 1. [4]

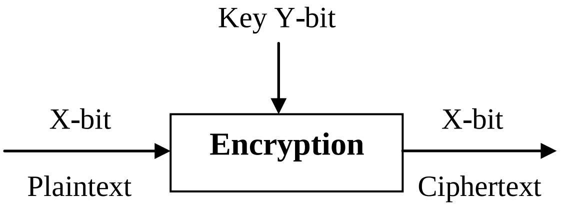


**Figure 1**- A block cipher

## 2. Previous Researches

1. In 2006, Alaa Khadem and Rehab F. Hassan introduce a new method to enhance the performance of the Data Encryption Standard (DES) Algorithm. This is done by building a new structure for the 16 rounds in the original algorithm. This structure makes use of multiple secrete keys working on 132 block size. The principle of Cellular Automata (CA) is used to generate these multiple keys in a simple and effective way. The proposed method provides high quality encryption, and the system is very resistant to attempts of breaking the cryptography key. [6]
2. In 2002, Nada Al-ubaidy depend on generated digital images cryptography to clip a symmetric block cipher keys with different lengths, the final images are established from combining two different separated patterns by using many mathematical methods. An additional technique is added to process the information by encrypt the encryption data more than one time with different keys and the decryption will be done easily.[7]

## 3. Why Graphical Image Generation

The old Chinese saying, “one picture is worth thousands words” can be modified in the computer age into “one picture is worth many kilobytes of data”.

It is natural to expect that graphical communication which is an older and more popular method of exchanging information than verbal communication will often be more convenient when computers are utilized for this purpose. This is especially true for a large number of engineering applications where one must describe objects in 2D and 3D spaces. Often it is much easier to display these objects on the screen than to attempt to visualize them from many pages of computer output describing their geometrical shapes [8].

There are two main reasons for the extreme usefulness of computer graphics for many applications:

- The first reason is that the computer graphic representation of information may be not only an appropriate but also the only reasonable method of handling information. This fact is tersely expressed by the saying” A picture is worth thousands words”.
- The second reason is given by the special kind of person-machine interaction that only computer graphics provides [9].

## 4. Fractal Geometry

Benoit B. Mandelbrot, who is often called the father of fractals, investigated the relationship between fractal and nature. He showed that many fractals existed in nature and could accurately model some phenomenon. He and his collaborators introduced many new types of fractals to model more complex things like trees and mountains. He furthered the idea of fractional dimension and later coined the term fractals from this revolutionary concept. [10]

Many theories and applications for fractals are just being discovered. 3D modelling of natural phenomenon is just one of the innovative technologies fractals have found their way into. Fractals are excellent at creating realistic images, because they can model natural objects well. [10]

The fractal is an irregular geometric object with infinite nesting of structure at all scales. The fascination that surrounds fractals has two roots:

1. The fractals are very suitable to simulate many natural phenomena, and
2. The fractal is simple to be generated on computers. [11]

The most amazing thing about fractals is the variety of their applications. Within the last 20 years, fractal geometry and its concepts have become central tools in most of the natural sciences and computer technology including computer graphics, biology field, chemistry, earth sciences, physics and fractal compression. [12]

In general there are two main types of fractals:

### a. Deterministic fractals

This type is the well known type of fractals, represented by the fractals that are composed of several scaled down and rotated copies of themselves. Julia set, Mandelbrot set and dust and cluster are some example of deterministic fractal. [13]

### b. Statistical Fractals (Random Fractals)

The statistical fractal was explained in one of the most important random fractals that used in 3D modelling objects is the plasma fractals (random midpoint displacement fractals) that are composed of several irregular recursive geometric shapes. [14]

To generate 2D image we used here diamond square brownian algorithm that merging between two strength algorithms that are diamond-square algorithm that make this image difficult to estimate and reproduce by the counterfeit, and brownian self-similarity algorithm that was found in plasma fractals and make the image more randomness by adding a random value for each pixel in the image. Diamond square algorithm taking the midpoints depend on points in four directions and add a random number to the average of this four points, the following Figure illustrates the mechanism of this algorithm for the first two iterations: [15]

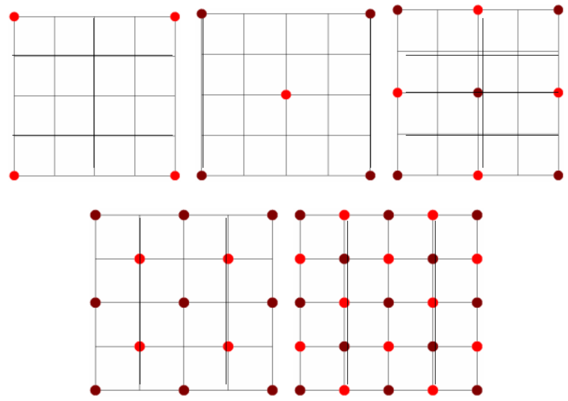


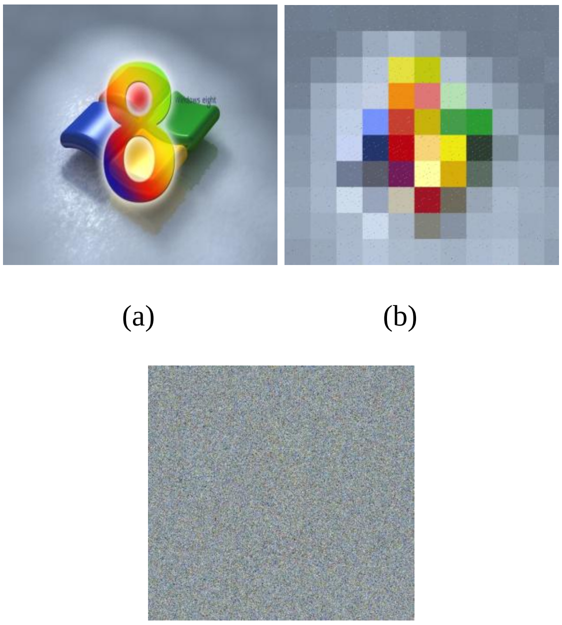
**Figure 2**- the points computed in the diamond and square steps

## 5. Fractal image generation

The final image is established by using diamond square algorithm and Brownian algorithm, this techniques gives opportunity to change the shape in an easy way to get different new patterns and then different pictures in any time with random colour (value) in each small area in the picture when compare this technique with the normal colour image we see in each small area the pixels have the nearest values. Three images are shown in figure (3), where the first one (a) is a normal colour image, while the second one (b) is the generated image drawn using diamond-square and the third one (c) is the generated image using diamond-square Brownian algorithm. Random values of RGB to each pixel also shown in Figure 3. It is clear from the nearest value from the first image and the randomness values from the third image.

The resulting image used to clip many different keys from her. (Each key is not depended on any of the other keys), by this way we obtained the cipher-text that have no depending to each other.

The clipped key from the generated image have the same length of the blocks of plain-text by this way we obtained non-repeating, keys with different lengths. We can use more than one message to encrypt by the same keys.



(a) (b)

(c)

**Figure 3**- Example for fractal image generation

## 6. Tests of Randomness to The generated 2D image

Different images are used in these tests and the results for the tests proved that the clipped keys have the randomness property and can be used as a symmetric key in cryptography field.
Table 1 show the results of randomness test for different lengths of 2D images.

**Table 1**- Randomness Test to an image in different size of bits.

| Test | | 64 bit | 128 bit | 256 bit | Pass Value |
|---|---|---|---|---|---|
| **Frequency test** | | **1** | **1.531** | **1.890** | **<= 3.84** |
| **Serial test** | | **1.968** | **2.523** | **2.356** | **<= 5.991** |
| **Poker test** | | **2.4** | **4.824** | **4.843** | **<= 43.77** |
| **Run test** | **T0** | **5.999** | **3.749** | **2.781** | **<= 9.488** |
| | **T1** | **7.999** | **8.187** | **9.562** | **<= 9.488** |
| **Auto correlation test** | **Shift1** | **4.372** | **0.103** | **1.845** | **≤3.48** |
| | **Shift2** | **0.114** | **0.356** | **0.826** | |
| | **Shift3** | **8.474** | **1.476** | **3.137** | |
| | **Shift4** | **2.604** | **1.030** | **0.018** | |
| | **Shift5** | **0.110** | **2.663** | **1.903** | |
| | **Shift6** | **1.396** | **0.642** | **0.804** | |
| | **Shift7** | **1.583** | **1.077** | **0.209** | |
| | **Shift8** | **1.798** | **1.608** | **0.538** | |
| | **Shift9** | **6.928** | **0.170** | **0.105** | |
| | **Shift10** | **1.380** | **0.407** | **0.318** | |

## 7. The proposed 3D-image generated using development of 2D mathematical models

This section, introduces a new idea to generate 3D-image by inserting a third coordinate (z) to all of the mathematical equations that were used to generate the 2D image. The value of x-axis and y-axis of the cube represent the vector and horizontal of the 2d image in sequence, where as the z-axis of the cube represent the location of the points.

Generating a 3D image is very useful to increase the key space, and make the process of estimating the key by the counterfeit infeasible. Because searching in three-dimensional increase the choices of estimating the control points for the counterfeit, and make the key more differentiable, effectiveness, randomness.

2D to 3D Image Converter takes an image (BMP or JPG format) and turns it into 3D.

To make the idea easy to be imagined when working with 3D, we suggest that the result fractal image divided into six pieces and put each piece on a one of the cube sides, and then clip slide from the cube that begin and end from a specific points.

The clipped slide from the three-dimensional image (3D) can be used directly as a secret key that used between the sender and receiver. The following Figure illustrates the proposed algorithm to generate 3D image that are used for clipping secure keys from it by a specific way.

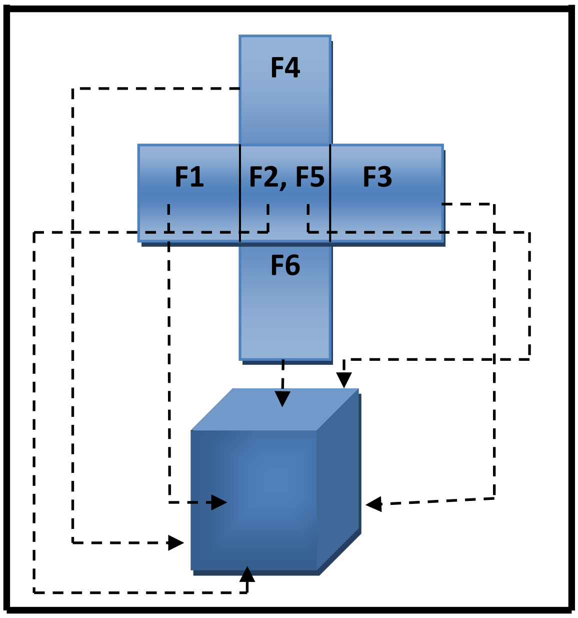


**Figure 4**- Generate 3D image [11]

## 8. Using Generated Digital Images by Mathematical Models in Cryptography

The weakness of the key that is generated From normal colour image is clear due to the nearest pixel value of image. A new method to generate cryptographic key proposed depending on generating (2D & 3D) images according to mathematical fractal algorithm that makes the key sufficiently robust.

A symmetric key is a string of random bits; simply the number of random bits in it measures the keys variability and strength. Cryptographers recommend that, to be reasonably secure, keys should be at least 90 bits long. The world standard is 128 bits because it is convenient size for computer. There is no technical reason to use a shorter key.

The size of the clipped key from the generated image is flexible depending on the flexibility of the generated image size, for example in the 2D-image, the image size used is

256×256 pixels that means it is equal to 65536 pixels each pixel represented by 24 bits. (i. e. the key size is 1572864 bits), and the key space that is used in 3D-image is (100×100×100) pixels which is equal to 1000000 pixels (i.e. the key space size is 24000000 bits). In this work, we clip samples of different keys sizes and test the randomness of the keys according to the five popular tests for the randomness. Figure 5 shows the proposed steps that are followed to get the ramdom keys from the image.

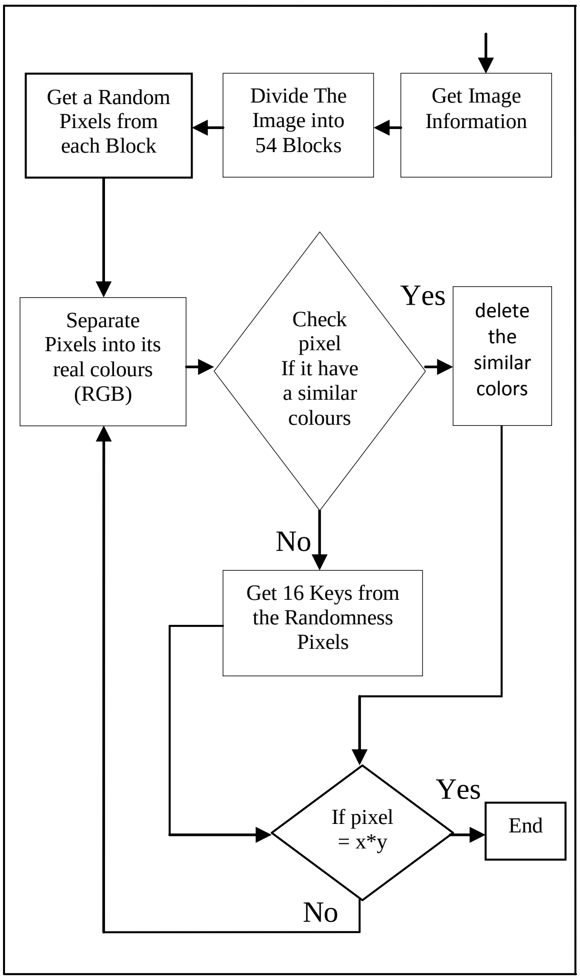

Get a Random Pixels from each Block
Divide The Image into 54 Blocks
Get Image Information
Separate Pixels into its real colours (RGB)
Check pixel If it have a similar colours
Yes
delete the similar colors
No
Get 16 Keys from the Randomness Pixels
If pixel = x*y
Yes
End
No

**Figure 5**- An Overview diagram of the proposed key generation steps

## 9. Symmetric-key Cryptography

Symmetric key systems require both the sender and the recipient to have the same key. This key is used by the sender to encrypt the data, and again by the recipient to decrypt the data. Key exchange is clearly a problem. How do you securely send a key that will enable you to send other data securely? If a private key is intercepted or stolen, the adversary can act as either party and view all data and communications. [16]

The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data.

Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys. [17]

Symmetric cryptography uses a single private key to both encrypt and decrypt data. Any party that has the key can use it to encrypt and decrypt data. They are also referred to as block ciphers.

Symmetric cryptography algorithms are typically fast and are suitable for processing large streams of data.

The disadvantage of symmetric cryptography is that it presumes two parties have agreed on a key and been able to exchange that key in a secure manner prior to communication. [16]

There are several types of symmetric algorithms used today. They have different methods of providing encryption and decryption functionality with two identical keys used to encrypt and decrypt the data. [2]

## 10. Data Standard Encryption (DES) cryptography

Simplified DES, developed by Professor Edward Chaefer of Santa Clara University. The algorithm is designed to encipher and decipher blocks of data consisting for 64 bits under control of a 64-bit key of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. Its output is 64-bit block of ciphertext. The following is a simple abstract about the encryption and decryption process of des algorithm. [18]

### a. Encryption process

The encryption process takes 16 rounds in which a round function, defined in terms the Sboxes, is applied over various subkeys of 56-bit input key, which are generated according to a well defined scheme. The diagram in Figure 6 shows the flowchart of DES.

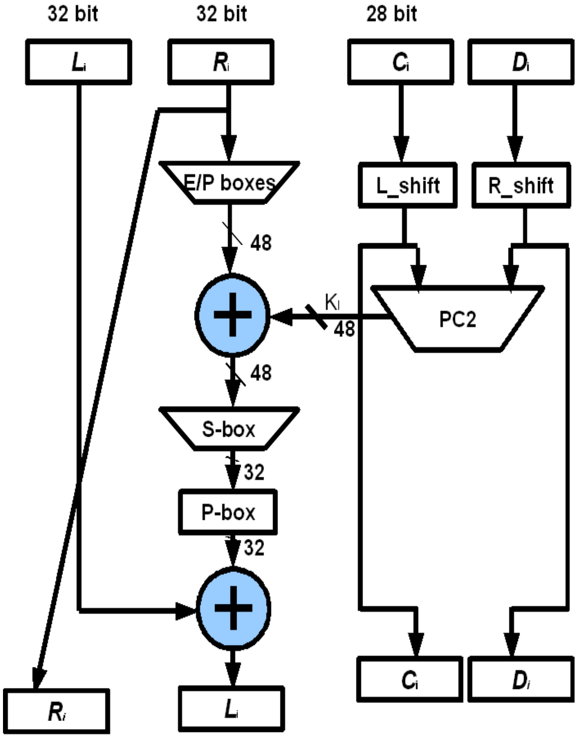


**Figure 6**- Data Encryption Standard Flowchart

First we introduce the following notations: Let *L(x)* denote the left half of a 64-bit string x, let R(x) denote the right half of x, and let C(x) be given by

$C(x) = R(x) \mid\mid L(x)$ ........................... *(1)*

In other words C(x) changes the right and left halves of x. We explain this algorithm in the following steps: [18]

**1.** An initial permutation, designated as IP, this applied to 64 bits of plaintext.

**2.** This bits is split into two 32-bit halves designated L(left) and R(right).

**3.** At the same time, the first subkeys K1, a 48-bit string is generated.

**4.** The subkey K1 analog with the right halve R are used as inputs to the round function F(K;R(x)) to produce a 32-bit output.

Blow we explain briefly the steps of the round function F:

- ❖ Expand x from 32 bits to 48-bit, by using the expansion box E.
- ❖ Apply the module 2 addition of E(x) and K, the output is also 48-bit.
- ❖ Where the later is concatenation of eight bit string Bi of length six, say $E(R(x)) \oplus K = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$.
- ❖ Enter each $B_i$ into S-box where S-box is generated from a linear function, which takes six bits as an inputs and get four outputs. Figure (8) illustrate the S-Box design.
- ❖ The output of the pervious step has a 32-bit length is entered into the permutation function P, which is defined as P box.

**5.** The output from the round function F is XOR-ed with the left half of the plaintext.

**6.** Finally, the left old half of the plaintext is replaced by the old right half, and the output of the XOR replaces the old value of R. The function f represents this step.

$f_k(x) = (L(x) \oplus F(k,R(x))||R(x)$ ...........*(2)*

Where

$f_k(x) = P(S(E(R(x))) \oplus L(x))$ ............*(3)*

**7.** This completes one round of the DES. The same procedure is applied 15 more times, the difference being the generating 3D image was used as a source for clipping keys, so the round function f has a different input subkeys to it every round. Notice that when FK16 is applied the right and left halves of the preoutput are not switched.

**8.** The last step of encryption is to reassemble the L and R output by the last round of fk16 of 64-bit string and apply the inverse of initial permutation IP-1.

**b. The Decryption Process**

DES has the feature that the decryption of the ciphertext produced with a key who corresponding subkeys are K1, K2,…,K16 is achieved by applying exactly the same algorithm that was used to encrypt except that the subkeys are used in reverse order K16, K15,…,K1.

Decryption takes 64-bit input of ciphertext analogy with a 56-bit key and produces a 64-bit output of plaintext. [18]

## 11. The proposed Algorithm

**Step-1:-** convert image into diamond square algorithm.

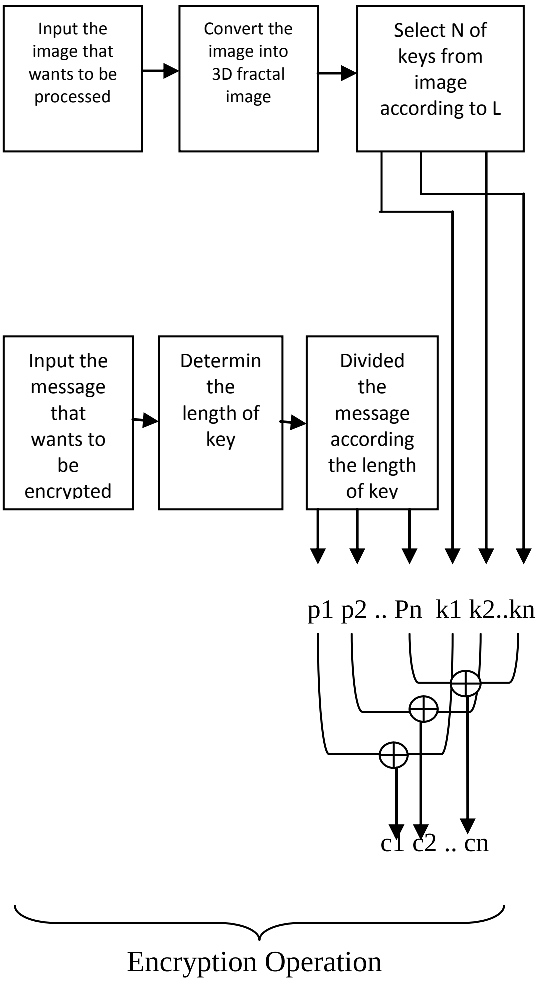
**Step-2:-** convert the result image from step1 into fractal.

**Step-3**:- convert the 2d fractal image that result in step2 into 3D image.

**Step-3:-** get randomness keys.

**Step-4:-** convert the plaintext into binary representation.
**Step-5:-** split the plaintext according the clipped key.
**Step-6:-** Each segment of the message is ciphered with different keys clipped from the image (using XOR), then the number of segment are equal to the number of the number of the counter and add one key to represent the reminder.
**Step-7:-** Merging the left part of the plaintext with the result of step6.
**Step-8:-** Rearrange the text by using IP-1 table.
**Step-9:-** Generate the ciphertext for one block.
**Step-10:-** If block = 0 then go to step11.
**Step-11:-** Go to step6.
**Step-12:-** Show the cipher text and end.

The following Figure illustrates the block diagram of the proposed system:


Input the image that wants to be processed
Convert the image into 3D fractal image
Select N of keys from image according to L
Input the message that wants to be encrypted
Determin the length of key
Divided the message according the length of key
p1 p2 .. Pn k1 k2..kn
c1 c2 .. cn
Encryption Operation

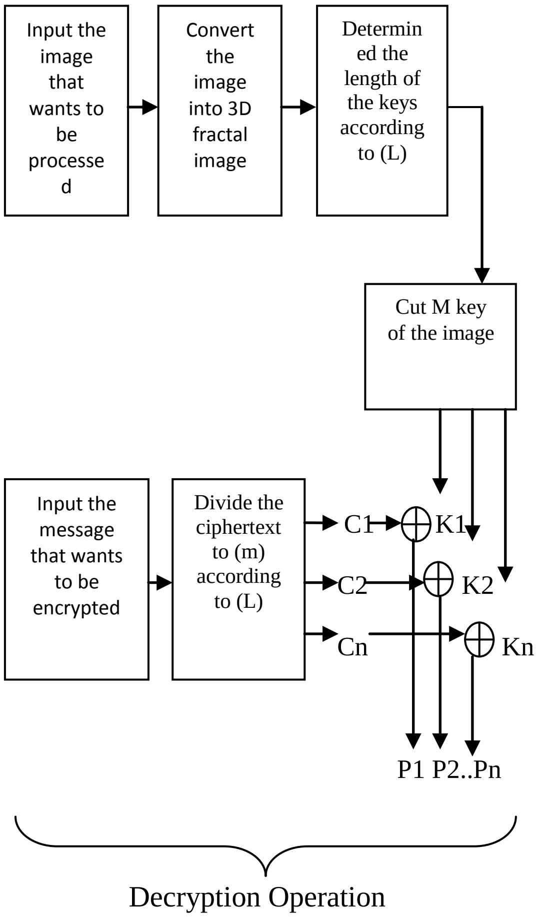

Input the image that wants to be processed
Convert the image into 3D fractal image
Determined the length of the keys according to (L)
Cut M key of the image
Input the message that wants to be encrypted
Divide the ciphertext to (m) according to (L)
C1
C2
Cn
K1
K2
Kn
P1 P2..Pn
Decryption Operation

**Figure 7**- the block diagram of the proposed system

**Example for encryption process:**

**Message:** BLOCK CIPHER ALGORITHM
**Key:** 564,401,13300991

**Ciphertext :** 1B 8E 49 3E 1C C3 03 01 61 43 B3 6F CC E7 4D CD 45 F0 93 6D 2C 36 56 6E F8 F2 EC A2 49 61 ED 42 0D F7 97 FF 09 3A ED 08

**Example for decryption process:**

**Ciphertext :** 1B 8E 49 3E 1C C3 03 01 61 43 B3 6F CC E7 4D CD 45 F0 93 6D 2C 36 56 6E F8 F2 EC A2 49 61 ED 42 0D F7 97 FF 09 3A ED 08
**Key:** 564,401,13300991

**Message:** BLOCK CIPHER ALGORITHM

## 12. Image Cryptography

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., to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access. [19].

Figure 8 shows the basic concept of image cryptography.

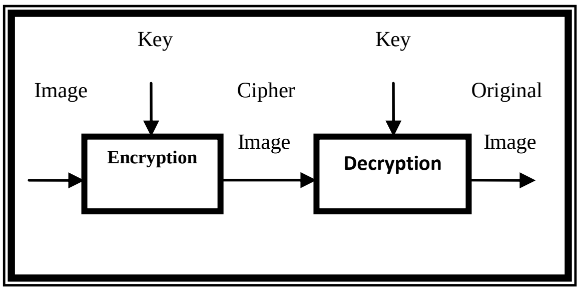
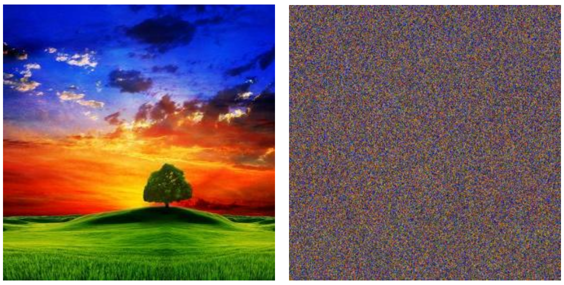


**Figure 8**- Image cryptography concepts

## 13. Implementation

The following examples of images show the results of implementing the Diamond-Square Brownian algorithm for encryption images on different JPEG images.

Original Image Ciphered Image



23.9 KB (24,497 bytes)

100 KB (103,324 bytes)

38.4 KB (39,351 bytes)

8.74 KB (8,950 bytes)

## 14. Discussion

A new system is proposed to modify DES algorithm by make the input key to this algorithm more strength and private and this is done by make the source of clipping this key from 3D image that generated using fractal algorithms, the resulting cryptographic key gives good result to obtain the very high randomness and differentiable private key that enhance the performance of DES algorithm.

## 15. Conclusion

This work presents a new system that combines 3D generation image and the cryptographic algorithms by clipping cryptographic key from 3D-mathematical models (digital images) that are generated using fractal generation methods. The clipped key gives randomness and a unique private key that is automatically generated.

## Reference

1. Bruce, S. **1997**. *Applied Cryptography*. Second Edition. Published by John Wiely & Sons. Inc.
2. Harris, S. **2011**. *Different Type Of Cryptography*. Fourth Edition. CISSP All-in-One Exam Guide. Published by McGraw-Hill companies.
3. Alfred, J.M. and Paul, V. C. and Scott, A. V. **2001**. *HandBook of Applied*

*Cryptograph*. Fifth Edition. Published by Boca Raton: CRC Press.

**4.** Monrose, F. and Michal, Q. and Wetzel, Q. **2001**. Cryptography Key Generation From Voice. Bell Labs, Lucent technologies. Murray Hill, New Jersey. USA.

**5.** Ayad, A.S. **2005**. Visual Partial Encryption Using Wavelet and Clock-Controlled Random Algorithm. PhD. Thesis. Ministry of Higher Education and Scientific Research in Computer Sciences. Baghdad, Iraq.

**6.** Khadem, A. and Hassan, R. F. **2006**. New Approach for Modifying DES Algorithm By Using Multiple Keys. University of Technology. Baghdad, Iraq.

**7.** Al-ubaidy, N. **2002**. Cipher By Image Processing. M.Sc. Thesis. University of Technology. Baghdad, Iraq.

**8.** Stalings, W. **2003**. *Cryptograhy and Network Security. (Principles and Practice)*. Published by Pearson Education. Inc.

**9.** Asthana, R. and Sinha, K. **1993**. *Computer Graphics for Engineers*. Published by Wiley Eastern Limited, New Delhi.

**10.** Mandelbrot, B.B. **1982**. *The Geometry of Nature*. Published by San Francesco, CA: Free man.

**11.** Szemla, L. **1999**. 3D models generator simulating a grow of n-atural objects for virtual reality. Published by CESCG, Institute for Computer graphic and Algorithm.

**12.** Vicsek, T. and Shlesinger, M. and Matsushita, M. **2003**. Fractals in natural sciences. published by E.Tv.S university, Hungary. office of Naval Research. USA and Chou university, Japan.

**13.** Tel, T. and Fulop, A. and Vicsek, T. **1989**. Determination of Fractal Dimension for Geometrical Multifractals. Published by Journal of Physics A 159, pp:155-166.

**14.** Turcotte, D. L. **1997**. Fractal and Chaos in Geology and Geophysics. Published by Cambridge university press.

**15.** Keith, S. December **2006**. Algorithms for Generating Fractal Landscapes. Published by Course Hero, Inc.

**16.** Malayeri A. D. and Abdollahi, J. **2009**. Modern Symmetric Cryptography methodologies and its applications. published by arXiv.

**17.** Abdul. Elminaam D. S. And Abdul Kader H. M. and Hadhoud M. M. **2009**. Performance Evaluation of Symmetric Encryption Algorithms. Communications of the IBIMA. Volume: 08, ISSN: 1943-7765.

**18.** Carl, M. and Stephen, M. **1982**. Cryptography: A New Dimension Computer Data Security. Published by John Wiely & Sons.Inc.

**19.** Beker, H. and piper, F. **1982**. Cipher System, the Protection of Communication. Published by Northwood Books Publications, London.

**20.** El-Zoghdy, S. F. and Yasser A. N. and Abdo A. A. **2011**. How Good Is The DES Algorithm In Image Ciphering. Int. J. Advanced Networking and Applications Volume: 02. Issue: 05.

**21.** Zenon, H. and Voloshynovskiy, S. and Rytsar Y. **1997**. Cryptography and Steganography of Video Information in Modern Communication. in Third TELSIKS97, Yugoslavia. pp:115-125.