Design and Implementation of a cryptographic system for images using Random number generator

Lecturer assistant . Jan syril fadhelalla
Market research and consumer protection center
Baghdad university

Abstract:

In the present work the design and development of ciphering method on colored images is studied. The method use incryption keys for ciphering and deciphering, where a random number generation program is used to produce a set of values that determine the incryption keys. In that mid point circles generating algorithmis used to locate a number of interrelated circles so as to determine the pixels to be ciphered.

1. Introduction:

If the word cryptography is heard, it is first associations might be e-mail encryption, secure website access, smart cards for banking applications or code breaking during world warII. Cryptography is a rather old business, with early examples dating back to about 2000 B.C., when secret hieroglyphics were used in ancient Egypt[1].

2. Cryptology

Cryptology splits into two main branches as in Fig(1):

1. Cryptography is the science of secret writing with the goal of hiding the meaning of a message[2].

Also the cryptography is divided into three main branches:

a – ymmetric Algorithms are what many people assume cryptography is about: two parties have an incryption and decryption method for which they share a secret key.

Symmetric ciphers are still in widespread use, especially for data incryption and integrity check of messages.

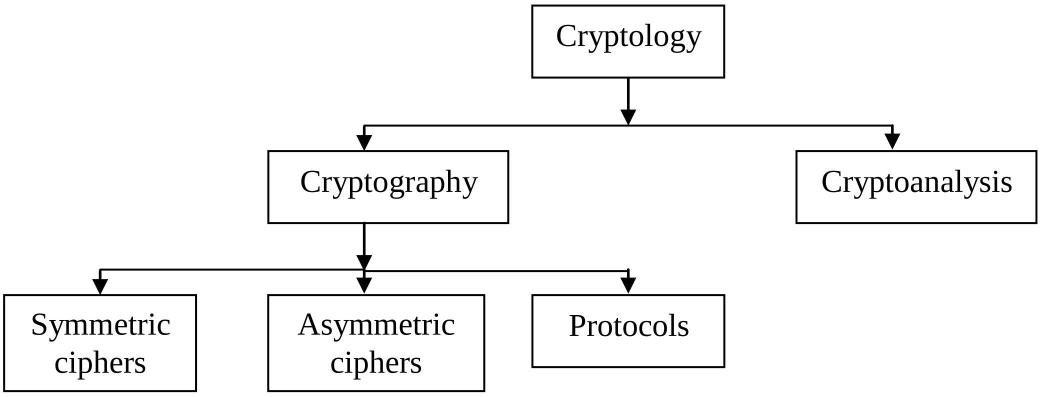
b- Asymmetric Algorithm:

A user processes a secret key but also a public key.

c- Cryptography protocols: Roughly speaking, crypto protocols deal with the application of cryptographic algorithms[3].

2. Cryptoanalysis: is the science of breaking cryptosystems.

Cryptoanalysis is of central importance for modern cryptosystems because: without people who try to break our crypto methods , we will never know whether they are really secure or not[3].

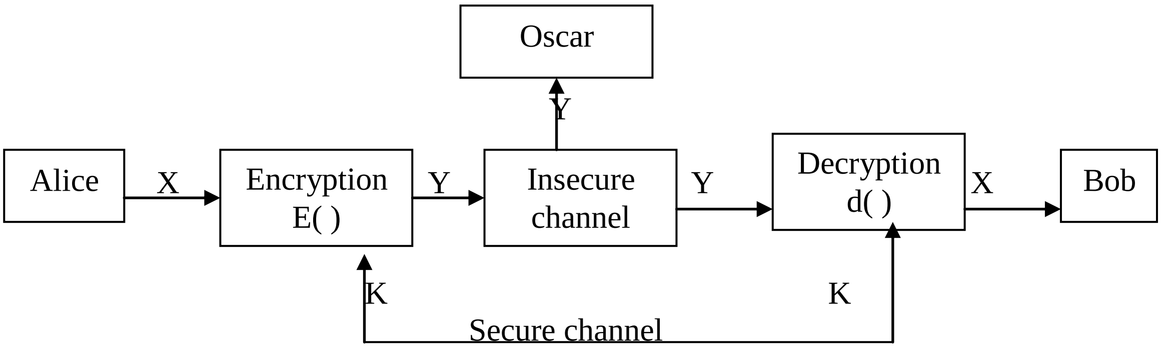


Fig(1), Over view of the field of cryptology[4]

2.1. Basics of symmetric cryptography

Symmetric cryptographic schemes are also referred to as symmetric key, secret-key, and single –key schemes or algorithms[5]. Symmetric cryptography is best introduced with an easy to understand problem: There are two users, Alice and Bob, who want to communicate over an insecure channel.The actual problem starts with the bad guy, oscar, who has access to the channel as in Fig(2).

In this situation, symmetric cryptography offers a powerful solution: Alice encrypts her message X using a symmetric algorithm, yielding the cipher text Y. Bob receives the cipher text and decrypts the message (inverse process of encryption).



Fig(2), Symmetric key crypto system

The variables X , Y and K in the figure above are important in cryptography and have special names:

- X is called plain text
- Y is called cipher text
- K is called the key
- The set of all possible keys is called the space[6].

3. The development method

3.1. Cryptographic Scheme

The symmetric cryptographic scheme is used in the designed system, where the same key is used for incryption and decryption.

The XOR operation is used in the process.

Assume that X XOR Y = Z
Then Z XOR Y = X

So if X is the plain text and Y is the key, then the resulted value of XOR operation Z is the cipher text which yields the plain text X if it is XORed with the same key K[7].

3.2. Choosing the keys

The goal of cryptamalysis is to find some weakness or insecurity in cryptographic scheme, thus permitting its subversion or evasion[8]. So choosing keys may be is usually effectively immune to cipher text attacks[9]. The random key generator program is used in the designed method so as to produce an infinite set of random numbers and to be manipulated with a specified factor value F. The random number function used generates the same set of numbers each time it is evaluated. This set of numbers will be used in designed method in certain way that will be discussed later.

3.3.The plain text

In the designed and implemented method, the plain text which is used is of image type, that is a sequence of pixels values. Chosen pixels are applied as operands to the XOR operator, in order to get the ciphered pixels.

3.4 Producing the cipher text

The following steps are applied to evaluate the ciphered image:

1. Lood the image to be ciphered.
2. Partition the image into a number of blocks of equivalent sizes.
3. For each block in the image file perform step 4 to 12.
4. Midpoint circle algorithm will be executed to produce the largest circle that may be included in the block with radius value R.
5. Repeat
6. Execute the random number generator to produce R1 that is to be manipulated with a specified constant factor to produce K. The value K will act as a key.
7. Apply the XOR operator for a pixel included in the generated circle and the key value K.
8. The resulted value is the ciphered pixel that is to be stored in the ciphered image.
9. Repeat step 6 – 8 for each pixel in the generated circle.
10. Decrease the radius R by 1
11. Locate the new circle pixels with radius R using midpoint circle generator.
12. Until R is less than or equal 2.

3.5. Retrieve the source image

The ciphered image is loaded and the steps of producing the ciphered image is activated in the same order to produce the source image, and using the same constant factor used in producing cipher text.

4. Results and Discussion

Many aspects appeared in the implementation of the designed method discussed as follow:

1. cryptonalysts try to break cryptography method, but that is difficult to be done with this method since the pool of keys is not predefined, where it depends on a random generation function and a specified factor.

2. All partitions of the image will be ciphered. Through the determination of the interrelated circles in all partitions of the image, and that is clearly found in Fig(4) and Fig(7).

3. Colors density does not affect the ciphered image since the ciphering keys are not fixed for all pixels. So the resulted ciphered pixels will be of different colors while the successive pixels in one partition of source image are usually of similar or nearly similar values, and that is clearly viewed in Fig(3) which consists of many different colors (pixels values), and in Fig(6) which consists of nearly similar colors(pixels values).

4. Decryption produces the source image again as can be seen in Fig(5) and Fig(8) which is similar to the source images Fig(3) and Fig(6) respectively.

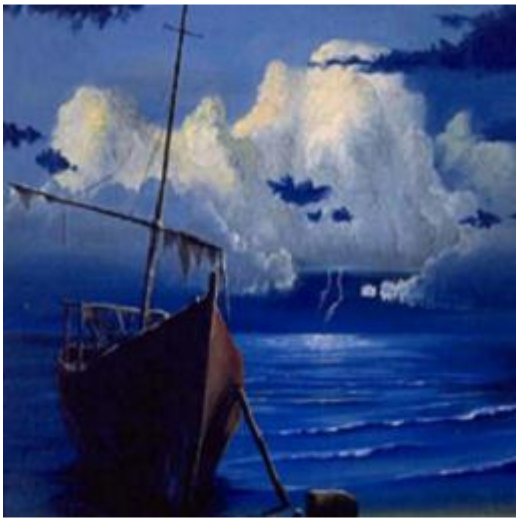
5. Conclusions

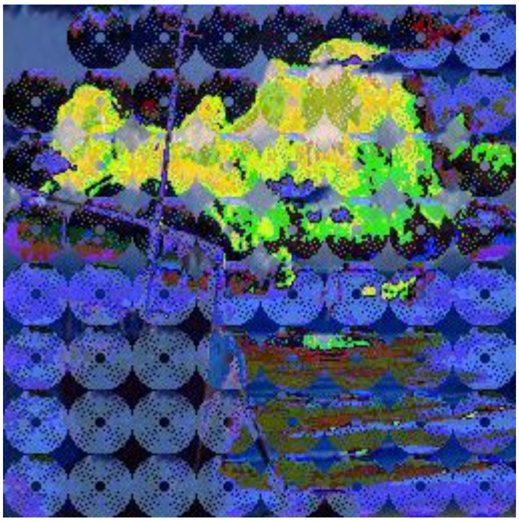
1. For images with some important features in certain blocks, the user may be asked to choose the blocks needed to be ciphered.
2. The factor value may be hidden in some place in the image (For example in the first block of the image).
3. Many other shapes may be used instead of circles, such as squares, rectangles, Triangles,……..etc.
4. The center of interrelated circles determined may not be the center of the block, so for each block the random number generator may be activated to determine a pixel dimensions that will act as a center for the interrelated circles(shapes used).
5. The sequence of blocks to be ciphered may be randomly chosen, that causes the croptoanalysis operation more difficult.

Output

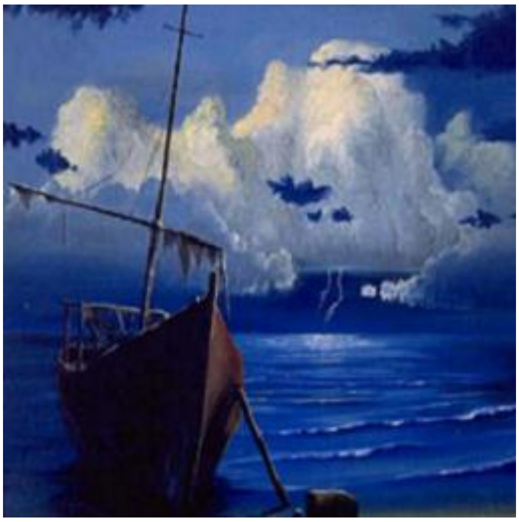
Here are examples of the output resulted from the project

Example 1



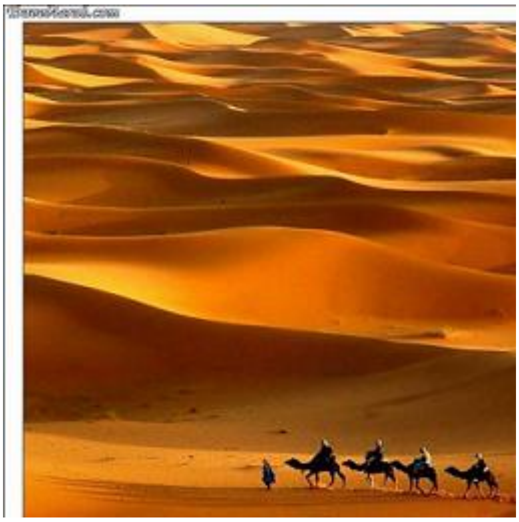


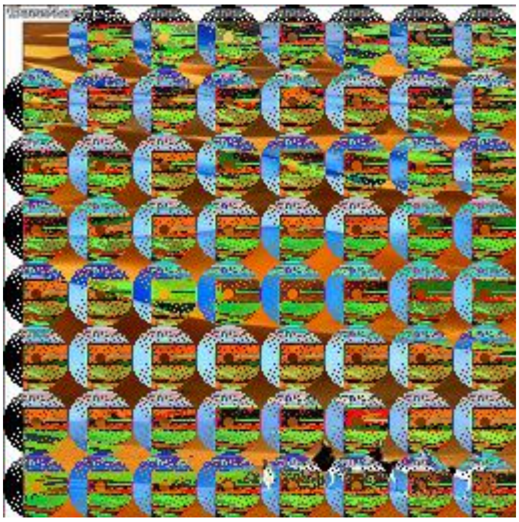
Fig(3), image before incryption Fig(4), image after incryption



Fig(5), image after decryption

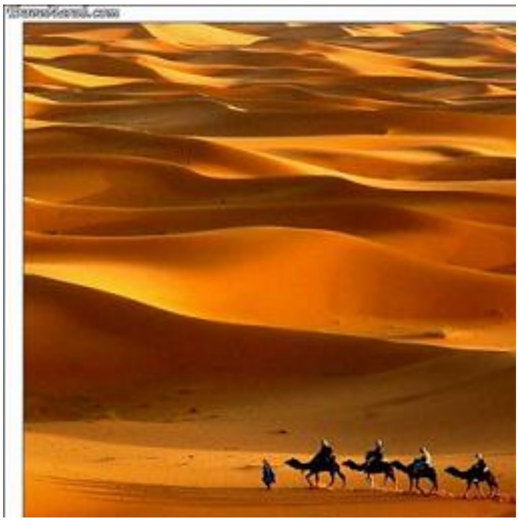
Example 2





Fig(6), image before incryption

Fig(7), image after incryption



Fig(8), image after decryption

References

1. Phil Zimme , ‘An Introduction to cryptography “, Kluwer Academic Publishers, 1998.
2. Andre Longie , “ Cryptography , A Study on Secret Writings “ , 1998
3. Philip R. Zimmerman , “Cryptography for the Internet” ,Scientific American , 1998.
4. John Wileys & sons Inc. Mark Stamp , “ Information Security Principles and Practice” , 2006.
5. Oded Goldreich, Prentice-Hall, “ Foundations of Cryptography “,2007..
6. Mihir Bellare , Phillip Rogaway , “ Introduction to Modern Cryptography”, Prentice – Hall ,2005.
7. John Wiley & Sons, Inc, Digital Design Preview Edition FRANK VAHID University of California, 2006
8. David F. Rogers , “Procedural Elements for Computer Graphics”, McGraw-Hill Book Company, 1985.
9. Mark T. Chapman , “Hiding the Hidden :A Software for Concealing Ciphertext as Innocuous Text” , A Thesis Submitted to the University of Wisconsin-Milwaukee , 2002.

تصميم وتنفيذ نظام تشفير للصور باستخدام مولد الارقام العشوائية

م. م. جان سيريل فضل الله
مركز بحوث السوق وحماية المستهلك
جامعة بغداد

الخلاصة

في هذا البحث تم دراسة تصميم واعداد طريقة لتشفير الصور الملونة. تستخدم هذه الطريقة نفس المفاتيح لاكمال عملية التشفير واعادة النص الاولي، حيث يتم الحصول على المفاتيح من خلال دالة انتاج الارقام العشوائية. حيث ان الاعداد العشوائية تعتبر كمفاتيح للتشفير. حيث يتم استخدام خوارزمية تكوين الدوائر لتحديد عدد من الدوائر المتداخلة التي تمثل نقاطها مواقع التشفير.