DESIGNING AN IMAGE CRYPTOGRAPHY SYSTEM USING THE IMAGE ELEMENTS AS CIPHERING KEYS

Dunia F. Saffo
Department of Computer Science, College of Science, University of Baghdad, Baghdad -Iraq.

Abstract

A design and implementation of images' cryptography system is evaluated in this paper. This system depends on the idea of allocating a part of a digital image (possibly the first block of the image) so as to produce the cipher keys for the other parts. Circles generating algorithm is used to produce keys from the chosen block, then corresponding circles in other blocks will be encrypted using the located keys. So in this method encryption keys are brought from the plain-image (source image) it self using graphics shapes pixels.

تصميم نظام تشفير للصور باستخدام عناصر الصورة نفسها كمفاتيح للتشفير

دنيا فضيل صفو

قسم علوم الحاسبات، كلية العلوم، جامعة بغداد، بغداد– العراق.

الخلاصة

تم في هذا البحث تصميم وإعداد نظام تشفير للصور. حيث يعتمد هذا النظام على فكرة تحديد جزء من الصورة الرقمية (وليكن الجزء الاول مثلا من الصورة) لاجل الحصول على مفاتيح التشفير للاجـزاء الاخرى. تم استخدام خوارزمية تكوين عناصر الدوائر لاجل تحديد مفاتيح التشفير من الجـزء الـذي تـم اختياره، ثم تحتسب دوائر مناظرة في الاجزاء الاخرى لاجل تشفير عناصرها باستخدام المفاتيح المحددة. وبهذه الطريقة فأن مفاتيح التشفير يتم جلبها من الصورة الاصلية نفسها وباستخدام عناصر اشكال الرسوم.

Introduction

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The primitives of cryptography should be evaluated with respect to various criteria such as: level of security, functionality, methods of operation, performance and easy of implementation [1]. Every few years, computer security has to re-invent itself. New technologies and new applications bring new threats, and forces us to invent new protection mechanisms. Cryptography became important when businesses started to build networked computer systems[2].

Cryptography enables you to store sensitive information or transmit it across in secure networks so that it cannot be read by anyone except the intended recipient where cryptography can be defined as, the science of using mathematics to encrypt and decrypt data [3].

Encryption Mechanism

The basic terminology of crypto includes the following:

-Cryptology is the art and science of making and breaking "secret codes".

-Cryptography is the making of "secret codes".

-Cryptoanalysis is the breaking of "secret codes", in order to obtain the meaning

of encrypted information. Typically, this involves knowing how the system works and finding a secret key.
Crypto is a synonym for any or all of the above [4].
Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such away as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. The process of reverting ciphertext to its original plaintext is called decryption [5].
A cipher or crypto system is used to encrypt data. A key is used to configure a cryptosystem for encryption or decryption. In a symmetric cipher the same key is used to encrypt or decrypt. The downside of symmetric encryption is that anyone who knows the secret key can transform the secret ciphertext to plaintext. This makes symmetric encryption vulnerable to leaking. Famous example of symmetric encryption used to be DES (Data Encryption Standard) which is no longer in wide use. There is also a concept of public key cryptography where the encryption and decryption keys are different, by so encryption is called public key encryption in which anyone can get the public key of the recipient to encrypt files or messages, so that only the holder of the private key of the public-private key pair can open the item. The downside of public key encryption is that asymmetric encryption usually is much slower and needs more computing power within any cipher [6]. The goal is to have a system where the key is necessary in order to recover the plaintext from the ciphertext. That is, even if the attacker, has to complete knowledge of the algorithms used and lots of other information, he cannot recover the plaintext without the keys [7].

Cryptography Systems

Cryptography systems are generically classified along three dimensions;
1. The type of operations used for transforming plaintext to ciphertext.
2. The number of keys used, and whether the system is symmetric or public.
3. The way in which the plain text is processed [8].

The Implemented Method

The cryptographic approach used in the implemented method is explained below along with the steps of implemented method for encryption and decryption.

1. Cryptography Approach

Symmetric key is used in the designed method, in which the sender and receiver will use the same key value for encryption and decryption, respectively.

2. Bit Manipulation Cipher

Bit manipulation ciphers convert source image into ciphered one by altering the actual bit pattern of each pixel through the use of a logical operator XOR. XOR is a binary operator that it will return true if one, and only one, of the two operators is true. The actual way exclusive-or encryption is used is to take the key and encrypt a file by repeatedly applying the key to successive segments of the file and storing the output. Once a second person has access to the key, that person is able to decrypt the file, but without it, decryption is almost impossible [9].

3. The Encryption / Decryption Implemented Method

The implemented method performs loading the image to be ciphered, cutting a part of this image, then this part will be used to generate keys for the encryption process to all other parts of the image itself. The keys are chosen through circles generating process. Interrelated circles will act as the chosen keys. The same keys will be used for retrieving the original image at the decryption process.

3.1 Production of Ciphered Image

The following steps are to be Performed to produce the ciphered image:
1. Load the image to be ciphered.
2. Partition the image into N blocks of equivalent size.
3. The first block will be selected to act as the pool of keys.
4. Use Midpoint circles generation algorithm [10] to determine the set of pixels composing a number of interrelated circles upon the selected block.
5. Pixels contained in the defined circles generated from step 4, are used as keys to encipher the corresponding pixels in other blocks of the image.

6.I=2
7.While I <= N do
7-1.Midpoint circles generation algorithm is applied upon

block I to determine the pixels composing a number of interrelated circles.
These determined elements are the pixels to be ciphered.
7-2 Repeat for each pixel in a generated circle in block I:
7-2-1 Apply the XOR operation for the two operands : the selected element from 7-1 and the key value that is produced in step 4 above, where the two operands are in corresponding locations in block 1 and block I.
7-2-2The result of the XOR Operation will reside as the new pixel value.
8.I=I+1
9.End while

3.2 Retrieval of the Original image

To retrieve the plain-image(source image), the following steps are to be performed:

1.Load the ciphered image, as it is received.
2.The image will be partitioned into the same number of blocks considered before encryption.
3.Mid point circle generation algorithm is applied upon the first block so as to determine a number of interrelated circles that contains the keys to be used for the decryption process.
4.I=2
5.While I <= N do
5-1 Mid point circles generation algorithm is applied upon block I to determine a number of interrelated circles. The pixels contained in these interrelated circles are the encrypted ones
5-2 Repeat for each pixel in a generated circle in block I.
5-2-1 Apply the XOR operation for the two operands: the selected element from step 5-2 and the key value that is produced in step 3 above, where the two operands are in corresponding location in block 1 and block I.
5-2-2 The output resulted from the XOR operation is the original pixel value.
6.I=I+1
7. End while

Conclusions

Some aspects appeared during the implementation and testing of the system:

1. Keys are difficult to be accessed by the analysts because it is brought from the same image and the selected block must be ciphered too as shown in fig.1-c and fig.2-c, and since there are multiple number of keys, so time required for analysis is equal to the number of blocks multiplied by the number of pixels contained in the interrelated circles generated in each block.
2. The pool of keys affect the ciphered image that is, contrastive colors in the selected block leads to a set of high differentiated keys which cause to disappearing the main properties of the image while low density of colors in the selected block leads to an image with the same main properties as the original one ,as shown in Fig.[2-b] , where the pool of keys is determined as the first block which consists of one color only.
3. The implemented method is not optimal to be used with images of little differentiated colors because the ciphered circles look to be approximately of one color, so that the main properties of the original image will remain in the encrypted image but with other colors as shown in fig [1-b], so this method is preferred to be used with images of high contrastive colors and for specified important parts of the image.
4. Execution time for the implemented method is practically not so far to the execution time measured for a number of encryption methods shown in table 1. Table 2 shows the execution time for the implemented method with equivalent environment used at the execution of the methods described in table 1.

Suggestions

Here are some aspects that may serve the implemented method if they are to be applied:

1. The block that serves as the pool of keys, may be chosen according to specific criteria for example the density of colors in that block, in this case information about the chosen block may be hidden in some location of the image.
2. Different graphic patterns may be used in order to represent the set of keys, as lines, rectangles, triangles,…etc.
3. Specified parts of the image may be ciphered (like human face), by giving the transmitter the chance to determine the blocks wanted to be ciphere. In the same manner, the receiver will choose the ciphered blocks only to perform the ciphering algorithm.

Examples

Figure 1-a: image before encryption.

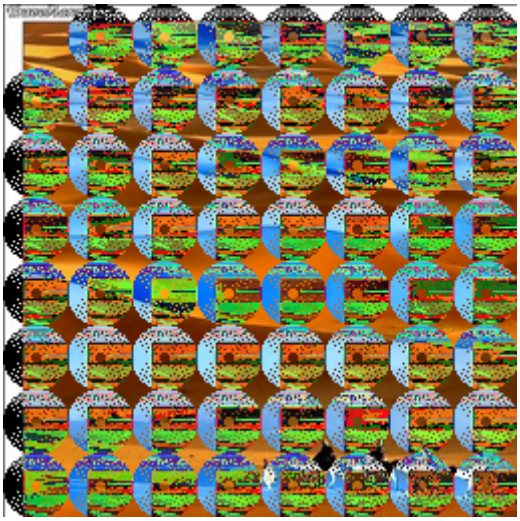

Figure 1-b: image after encryption.

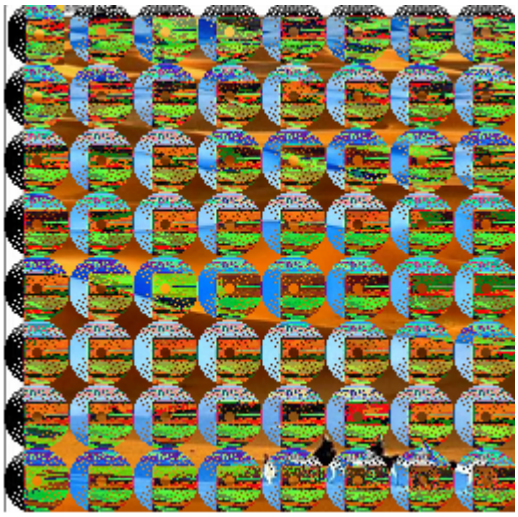

Figure 1-c: image after encryption of all blocks

Figure 2-a: image before encryption

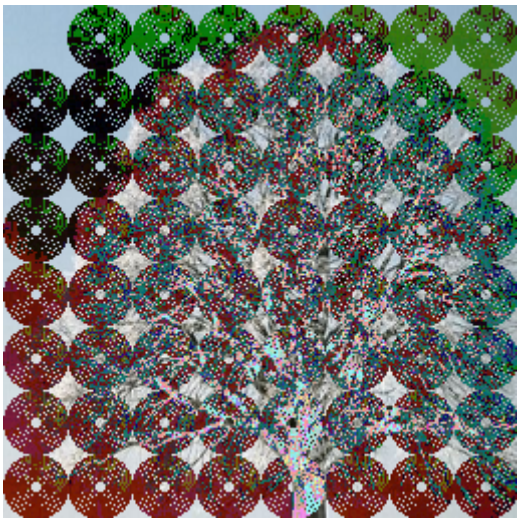

Figure 2-b: image after encryption of Blocks 2..n

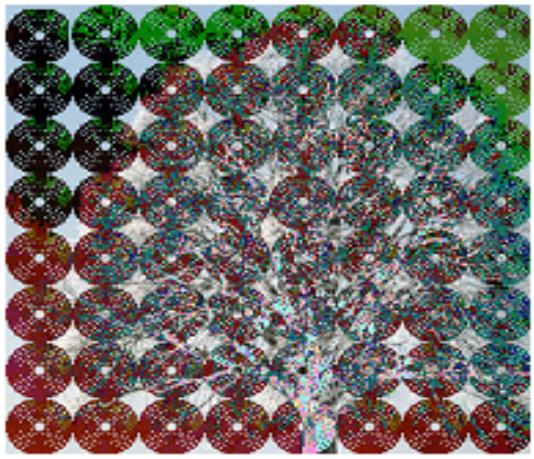

Figure 2-c: image after encryption of all blocks

Table 1: Comparative execution times (in seconds) of encryption algorithms [11].

Input Size (bytes)	DES	3DES	AES	BF
20,527	24	72	39	19
36,002	48	123	74	35
45,911	57	158	94	46
59,852	74	202	125	58
69,545	83	243	143	67
137,325	160	461	285	136
158,959	190	543	324	158
166,364	198	569	355	162
191,383	227	655	378	176
232,398	276	799	460	219

Table 2: execution time (in seconds) of implemented encryption algorithm.

Input Size (bytes)	Implemented method
20,527	45
36,002	84
45,911	110
59,852	145
69,545	158
137,325	295
158,959	348
166,364	378
191,383	418
232,398	488

References

1. Zimme, P. **1998**. *An Introduction to cryptography*. Kluwer Academic Publishers. pp. 21-23.
2. Stamp, M. **2006**. *Information Security Principles and Practice* , John Wileys and sons Inc. pp. 40-42
3. Zimmerman, P. R. **1998.** *Cryptography for the Internet*. Scientific American. pp.120-131.
4. Petitcolas, F. A. P. and Anbeisser S. K. **2000**. *Information Hiding Technique for Steganography and Digital Watermarking*, Artec house Inc. pp 80-88.
5. Longie, A. **1998**. Cryptography, A Study on Secret Writings. Prentice-Hall. pp.12-14.
6. Goldreich, O**. 2007**. *Foundations of Cryptography* , Prentice-Hall.pp.31-34.
7. Bellare, M. and Rogaway, P**. 2005**. *Introduction to Modern Cryptography*, Prentice – Hall .pp 31-45.
8. Bellare, M. and Sashay. **1999**. Non-Malleable Encryption :Equivalence between Two Notions, and Indistinguishability-Based Characterization, In Crypto'99,LNCS 1666, ,Springer-Verlag, Berlin. pp:519-536.
9. Chapman M. T. **2002**. Hiding the Hidden: A Software for Concealing Ciphertext as Innocuous Text", M.Sc. Thesis Submitted to the University of Wisconsin-Milwaukee, pp.13.
10. Schneider P. and Eberly D. **2002**. *Geometric Tools for Computer Graphics*. pp.50-54.
11. Nadeem, A. et al **.2005**. A Performance Comparison of Data Encryption Algorithms, *IEEE*.