Scramble Image Based on LFBSR (Linear Feedback Shift Registers)

Ghassan Muslim Hassan

Baghdad-Iraq

Mustansiriyah University/College of Sciences/Computer Department

E-mail: gmhalsaddi@yahoo.com

المستخلص

إحدى الطرق للحفاظ على امنية ارسال الصورة هي البعثرة، والتي تعني نثر او اعادة ترتيب مواقع نقاط الصورة (pixels) بطريقة بحيث يصعب تمييز الصورة الاصلية. الطريقة المقترحة في هذا البحث هي باستخدام مسجلات الازاحة وبوابات الـ XOR، بحيث نحصل على صورة مبعثرة جيدة باستخدام بعض الاختبارات والتي تم تطبيقها على النتائج. كما يمكن تطبيق الخوازمية بصورة فورية على الصورة كما ان التطبيق سهل جدا عند متابعة الخوازمية.

الكلمات المفتاحية

الصورة المبعثرة ، مسجلات الازاحة ، التبادل ، المخطط الاحصائي

Abstract

One way of security is Image Scrambling. Scramble in general mean, scattering all elements in a random ways. Scatter the pixels of any image in the way that which can't recognize the image, that is called "Image Scramble". There are many types of image scrambling. The proposed method in this paper deals with a series of shift registers and using XOR gates. The scrambled image having good security by using many tests of the results. The proposed algorithm can applied to the images in a real-time applications, and the implementation is easily done.

Keyword

Scramble image; Shift register; Exchange; Histogram

1. Introduction

The rapid growth of computer networks allowed large files, such as text, audio, and images, to be easily transmitted over the internet and it is important to protect the confidentiality of image data from unauthorized access [1]. The information security becomes an important and urgent issue not only for individuals but also for business and governments[2]. Security of image and video data is very important in many areas, such

as privacy, security communication, and also in military applications. Image scrambling is a good tool to make the scrambled image visually unrecognizable and difficult to decrypt for unauthorized users.[2]
In telecommunications and recording, a scrambler (also referred as a randomizer) is a device that manipulates a data stream before transmitting. The manipulations are reversed by a descrambler at the receiving side. Scrambling is widely used in satellite, radio relay communications [3]. A scrambler replaces sequences into other sequences without removing undesirable sequences, and as a result it changes the probability of occurrence of vexatious sequences[3].

2. Purposes of Scrambling

There are two main reasons why scrambling is used:[3]

- It facilitates the work of a timing recovery circuit, an automatic gain control and other adaptive circuits of the receiver (eliminating long sequences consisting of '0' or '1' only).
- It eliminates the dependence of a signal's power spectrum upon the actual transmitted data, making it more dispersed to meet maximum power spectral density requirements (because if the power is concentrated in a narrow frequency band, it can interfere with adjacent channels due to the cross modulation and the intermodulation caused by non-linearity of the receiving tract).

3. Types of Scrambling

3.1 Additive (Synchronous) Scramblers

Additive scramblers are also called synchronous (because they require the initial state of the scrambler and descrambler to be the same) or non-recursive (because they do not have feedback loops)[4]. A sync-word is a pattern that is placed in the data stream through equal intervals (that is, in each frame). A receiver searches for a few sync-words in adjacent frames and hence determines the place when its LFSR must be reloaded with a pre-defined initial

state[3][4]. The additive descrambler is just the same device as the additive scrambler, figure (1);

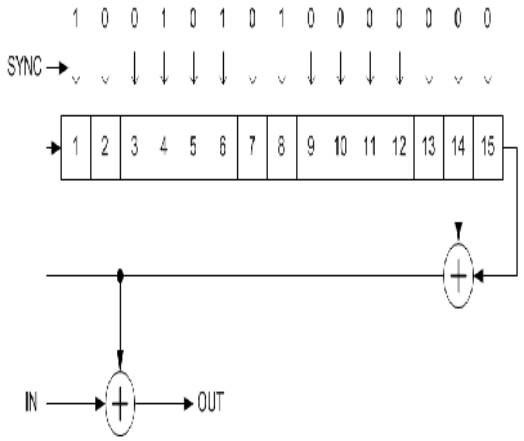

Figure (1) An additive scrambler (de-scrambler)

Additive scrambler/descrambler is defined by the polynomial of its Linear Feedback Shift Register (LFSR), for the scrambler on the figure (1), with its initial state.

$$1 + x^{-14} + x^{-15} \quad \ldots\ldots\ldots\ldots (1)$$

3.2 Multiplicative (Self-Synchronizing) Scramblers

Multiplicative scramblers (also known as feed-through) are called so because they perform a multiplication of the input signal by the scrambler's transfer function . A multiplicative scrambler is recursive and a multiplicative descrambler is non-recursive. Unlike additive scramblers, multiplicative scramblers do not need the frame synchronization, that is why they are also called self-synchronizing. Multiplicative scrambler/descrambler is defined similarly by a polynomial (for the scrambler, figure (2)); which is also a transfer function of the descrambler figure (3);[3][5]

$$1 + x^{-18} + x^{-23} \quad \ldots\ldots\ldots\ldots (2)$$

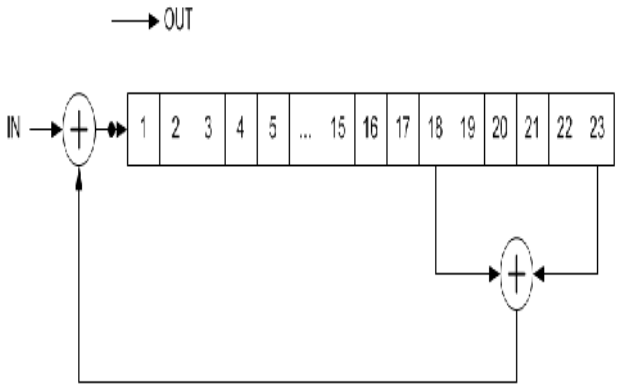

Figure (2) Multiplicative scrambler

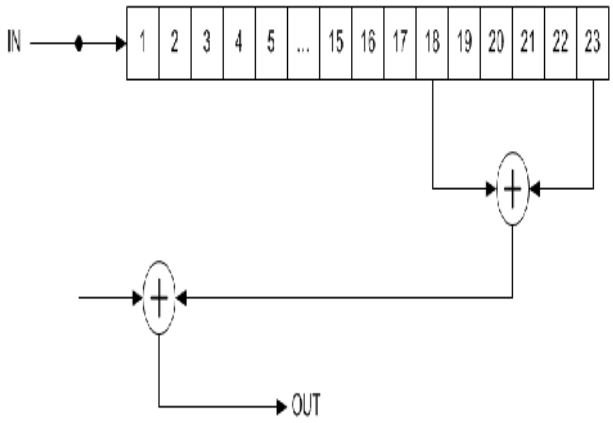

Figure (3) Multiplicative de-scrambler

4- Image Representation

Images are represented as a digital, where it was obtained as a result of sampling and quantization of an analog image or created already in digital form. It can represented as a two dimensional (2D) matrix of numbers.[6]

4-1 Binary (1-bit) Images

Binary images are encoded as a 2D array, using 1-bit per pixel, where a “0” means “black”, and “1” means “white”.[6]. The main advantage of this representation suitable for images containing simple graphics, text, or line art[6], figure (4);

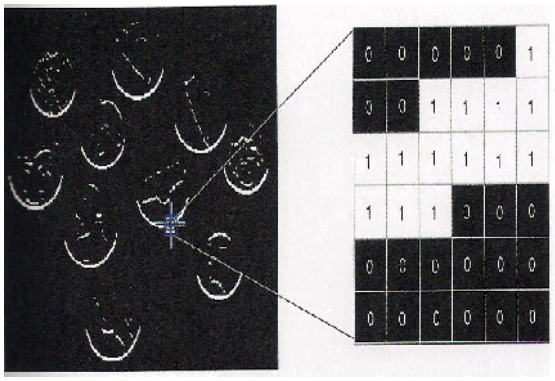

Figure (4), A binary image and pixel values in 6x6 neighborhood

4-2 Gray-Level (8-bit) Images

Gray-level images are encoded as a 2D array of pixels, with 8-bits per pixel, where a pixel value of “0” corresponding to “black”, a pixel value of 255 means “white”, and intermediate values indicate varying shades of gray.[6], figure(5).

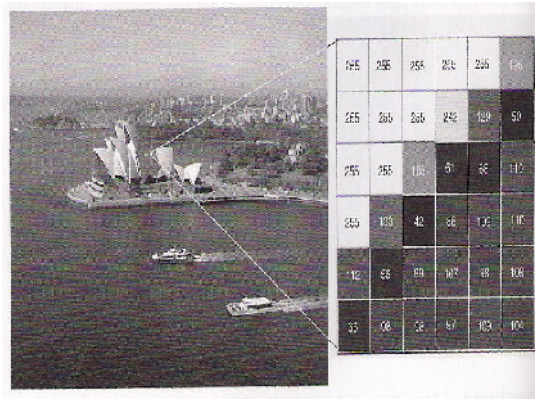

Figure (5), A gray scale image and the pixel values in 6x6 neighborhood

4-3 Color Images

Representation of color images is more complex and varied[6]. The two most common ways of storing color images contents are RGB representation(red, green, and blue). Using the 8-bit monochrome standard as a model, the corresponding color image would have 24bit/pixel (8-bit for each color bands). The second way

is indexed representation, where 2D array contains indices to a color palette[6,10]. Figure (6).

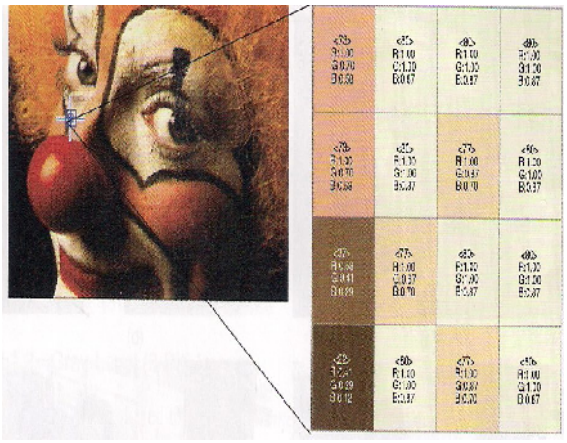

Figure (6), An indexed color image and the indices in 4x4 neighborhood

5- Scramble Algorithm

The proposed algorithm uses a shift registers and XOR gates to get scramble image. The algorithm divided in two parts, one for scrambling, and another for descrambling.

5-1 Scramble Algorithm

Step 1: Load the plain image , put it in an array

Step 2: Get width and height of the image (row & column)

Step 3: Iterate from 1 to number of rows.

Step 4: Iterate from 1 to number of columns.

Step 5: If row = column = 1

{

Exchange “0” and “1” ;

Change between the bits of first pixel ;

}

Else

If column ≠ 1

{

XOR between some bits ;

Change between the bits of a pixel ;

}

Else

{

XOR between some bits ;

Change between the bits of a pixel ;

}

Step 6: Put the result in another array

Step 7: Draw the scramble image

5-2 De-scramble Algorithm

Step 1 : Load the scramble image, put it in an array

Step 2 : Iterate from number of rows to 1.

Step 3 : Iterate from number of columns to 1.

Step 4: If row = column = 1

{

Change between the bits of first pixel ;

Exchange “0” and “1” ;

}

Else

If column ≠ 1

{

Change between the bits of a pixel ;

XOR between some bits ;

}

Else

{

Change between the bits of a pixel ;

XOR between some bits ;

}

Step 5: Put the result in a new array

Step 6: Draw the descramble (plain) image

6- Results & Security Test

In this section many tests was done due to the result of main program by using MATLAB programming, and performance of the proposed scramble image is analyzed in details.

6-1 Test of Visual

About seventy images are scrambled by the proposed method, then the visual test is performed. Figure (7) shows examples of the plain image and the scramble one, where the plain images are with many m*n pixels, even with color or gray images. There are no visual information observed in scramble image if the comparison was done between plain and scramble images.

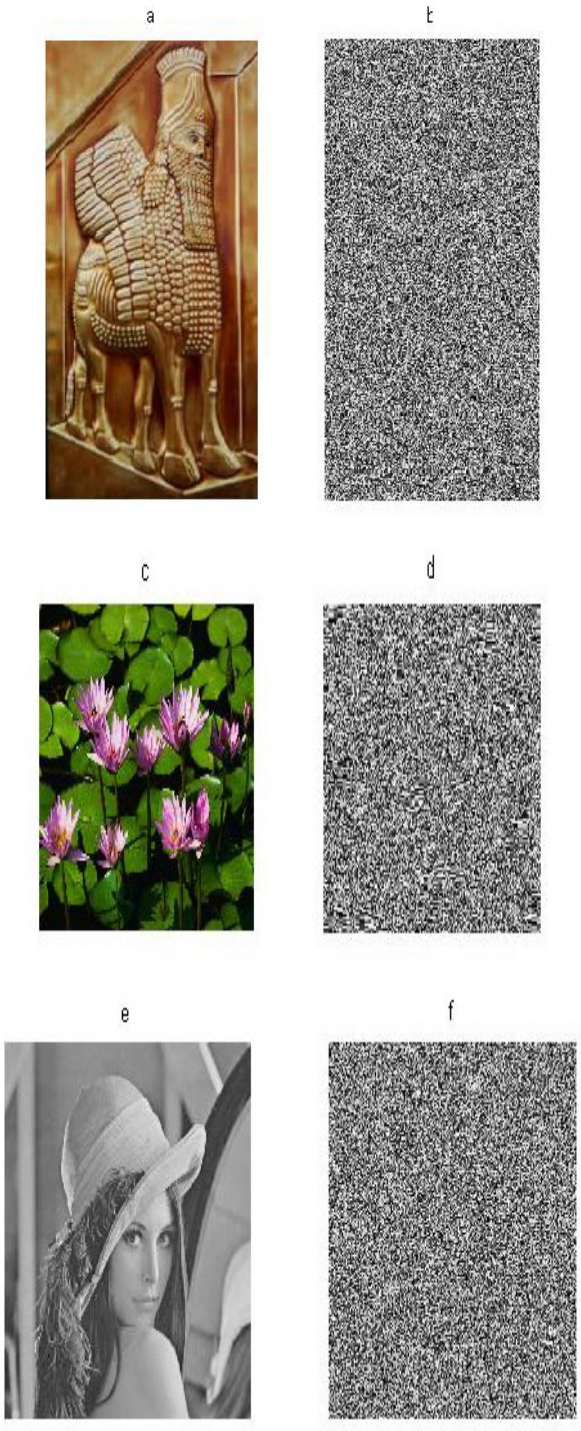

Figure (7) Examples of plain images (a,c,and e) and scramble images (b,d, and f)

6-2 Stable Points of Scrambling

The stable points means that point(s) which remain constant (the same) even if the scrambled was done, e.g. if the pixel numbered as "150", which equal to "10010110" (in binary format), and if the change like this : 1 4, 2 8, 3 5, and 6 7. After scramble,

the sequence of bits remain the same (“10010110”), that’s mean the stable point was exists.

The seventy images which converted by proposed method of scramble lead to table(1), which deals with stable points of images.

Stable points of 70 images	minimum	maximum
	0.22%	0.48%

Table (1) statistical results of stable points

for about 70 images after scrambling

the statistical results shows that the percentage of the stable points for 0.22% ~ 0.48% (even some images has more than 70000 points) in whole points, which are considered a very few.

6-3 Analysis of Histogram

> In statistics, a histogram is a graphical representation showing a visual impression of the distribution of data. It is an estimate of the probability distribution of a continuous variable[7].

If there is any statistical similarities between plain and scramble image, then the technique was failed. So by using histogram analysis to clarifies that how the pixel values of image are distributed. Figure (8) illustrate the histogram analysis of the images in figure(7), by using red channel of the plain image and the scramble image, figure(8) do not show any similarities.

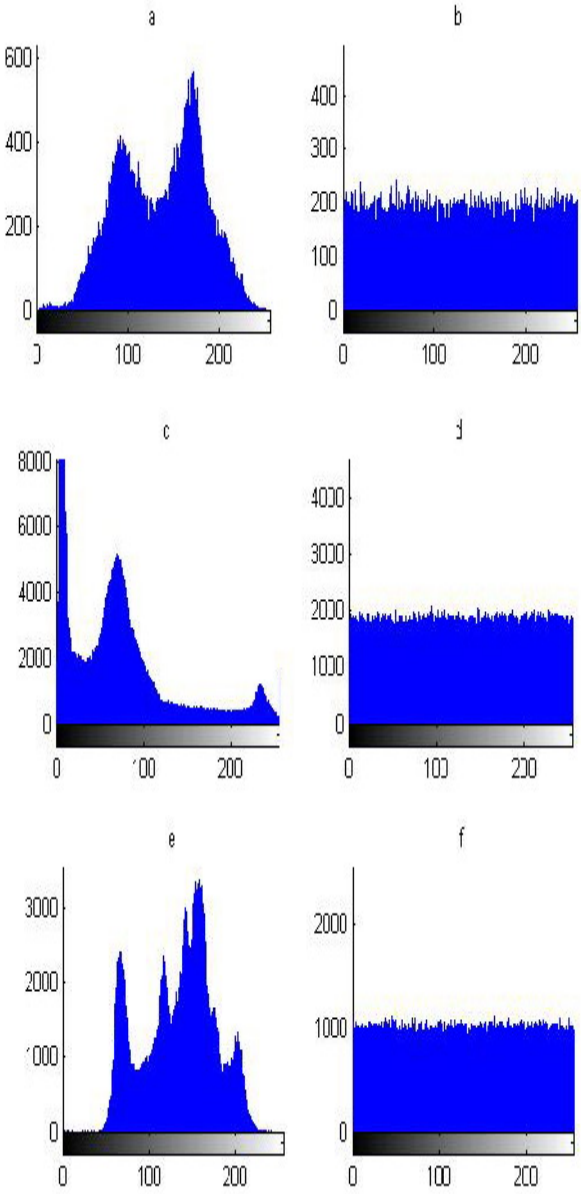

Figure (7) A histogram of plain images (a,c,and e), and scramble images (b,d, and f)

6-4 Neighbor Pairs

The Neighbors pairs mean that, a two pixels (points) are successive in plain image, also successive in scramble image after applying scrambling.

The two neighbor points may be horizontally or vertically adjacent. This is the nature of ordered pairs for each 3x3 sub-images. Let a pixel P at coordinates (x,y), then the neighbors of P from 3x3 sub-image is : (x+1,y),(x-1,y),(x,y+1),(x,y-1).[8]. Figure(9)

x-1,y-1	x-1,y	x-1,y+1
x,y-1	x,y	x,y+1
x+1,y-1	x+1,y	x+1,y+1

Figure(9) 3x3 sub-image with 8-neighbor

If the number of neighbor pairs are few, then the good effective are the method, and give a strong security to the proposed method. Again, more than 70 images are tested for this test, and some of the images have more than 70000 points (with 3x3 sub-image). Table (2), shows the statistical result;

Neighbor pairs	Minimum	maximum
Of 70 images	4.37%	7.14%

Table (2) statistical results of neighbor pairs for about 70 images with 3x3 sub-image, after scrambling

the statistical results shows that the percentage of the distribution pairs for 4.37% ~ 7.14% (even some images has more than 70000 points) in whole points, which are considered few and mean there is a good scramble method and then a good security.

7- Conclusion

The unauthorized person, is one who want to get the information illegally (image is one of this information). Many of techniques was made to prevent this scheme. This paper deal with this problem and put an algorithm to secure the image, which is based on shift register and many of XOR gates. The obtained results show that the scramble

image is unrecognized, so it help from those unauthorized person. In another way the descrambled images does not exactly the same when we compared with the plain image. Even if there is a small error, then it be acceptable

Reference

[1]W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images", Pakistan Journal of Information and Technology. Vol. 2, no. 2, 2008, pp. 191-200. http://www.ansinet.org

[2]YICONG ZHOU, KAREN PANETTA, FELLOW, IEEE, SOS AGAIAN, SENIOR MEMBER, IEEE, “An Image scrambling Algorithm Using Parameter Based M-Sequences”.