A NEW FUZZY PN CODES BASED COLOR IMAGE ENCRYPTION TECHNIQUE

Said E. El- Khamy[1], *Fellow IEEE*, Mona Lotfy, and Adel Hamdi Ali[2]

Electrical Engineering Department, Faculty of Engineering,
Alexandria University. Alexandria 21544, Egypt.
[1] elkhamy@ieee.org , [2] adel_Hamdi@alexandria.cc

Abstract — In this paper, a new image encryption system is proposed, in this system we use 4 binary sequences generated using a fuzzy PN bit generator recently developed by the authors to encrypt the image pixels. According to these sequences, each pixel color byte value will rotated as bits in right or left direction for some bits, after rotation process the pixel color will be XOR-ed by one of binary sequences. Finally, we obtain a highly encrypted image as shown in results.

1. INTRODUCTION

The wide use of digital data forms in transmission and storage, and the threat of illegal data access; data security has become a significant subject [1]. Encryption techniques [2] and watermark embedding schemes [3, 4] are proposed, to protect data against unauthorized readers and illegal reproduction, respectively.

A new color image encryption system is presented in this paper. The encryption algorithm is of combination form type where the image pixels are position permutated and value transformed randomly according to PN binary sequences [5]. The system uses a *Fuzzy Bit Generator* (FBG), recently developed by the authors [10], for generating binary sequences used in the encryption algorithm. Four binary sequences are used for image encryption. For algorithm simulation a VISUAL BASIC program is developed, the encrypted image disorder is measured visually and by the fractal dimension.

The recently developed fuzzy PN bit generator used in the encryption process is described briefly in section 2. In section 3, the new image encryption system is proposed. In section 4, the properties of the system are examined and simulation results are given. Finally, in section 5 is the paper conclusion.

2. RECENTLY DEVELOPED FUZZY BIT GENERATOR

In reference [10], a new method for generating pseudo-random (PN) binary sequence based on fuzzy logic has been presented. A learning procedure is applied to copy the behavior of real random source. The system generates pseudorandom binary sequences. The generated fuzzy binary sequences successfully pass all standard randomness tests and their length can be made arbitrary long. Such sequences are suitable for data encryption and secure direct-sequence (DS) spread-spectrum (SS). The use of the developed fuzzy binary generator to generate code families with good auto and cross correlation properties is also described in this paper. Although the generated codes appear to be random and enjoy most of the properties of random codes, they are deterministic. In other words, they can be exactly regenerated by fixing the parameters of the fuzzy random number generator.

On the other hand, by changing the initial condition for this system we obtain a new binary sequence. The fuzzy system rules are constructed using numerical data pairs during the training stage then combined with linguistic information to form the working it-then rules.

3. THE NEW IMAGE ENCRYPTION TECHNIQUE

Let $f(n,m)$ denote a pixel color of an image f of dimensions $N{\times}M$, where $n=0...N$-1, $m=0...M$-1. The encryption algorithm depends on two procedures, the first is for pixels permutation, and the second is for pixels value transformation. Providing 4 seeds for the FBG, we generate 4 binary sequences S_0, S_1, S_2, S_3 of length $N*M*12$.

3.1 Permutation Procedure

According to image dimensions, we will use the bits of S_0, S_1 to get the coordinate of the upper left corner of a 4×4 pixel blocks B_i of the image under encryption x_i and y_i .S_2 , S_3 are used to get the coordinates x_{i+1} and y_{i+1} for B_{i+1}.

Having theses randomly chosen blocks, we calculate the variance σ^2_i and σ^2_{i+1} [11]. The value of the variance will be used in the following permutation scheme.

```
Start
  Case $\sigma^2_i = \sigma^2_{i+1}$ : $B_i \leftarrow B_{i+1}^T$, and $B_{i+1} \leftarrow B_i^T$
  Case $\sigma^2_i > \sigma^2_{i+1}$ : $B_i \leftarrow B_{i+1}$, and $B_{i+1} \leftarrow B_i^T$
  Case $\sigma^2_i < \sigma^2_{i+1}$ : $B_i \leftarrow B_{i+1}^T$, and $B_{i+1} \leftarrow B_i$
End
```

$i= 1,...,X.$ where X is an arbitrary number of blocks. Fig. 1(a) shows a permuted image.

3.2 Value Transformation Procedure

In this procedure, three of the generated sequences will be used in the encryption process of the R, G, and B colors. The fourth will be used for controlling the swapping operation of sequences which will be shown later (section 3.3).

For each pixel we get 12 bit from each sequence, so we will have 12*4=48 bit for encrypting one RGB pixel. The pixel color value will be rotated in a direction *Dr*, for a number of positions *NRP*, and then Xored with a value *XoR* .

$$Dr_x = \begin{cases} left : S_z(0) = 0 \\ right : S_z(0) = 1 \end{cases} \tag{1}$$

$$NRP_x = \sum_{i=0}^{2} S_z(i+1) \times 2^i \tag{2}$$

$$XoR_x = \sum_{i=0}^{7} S_z(i+4) \times 2^i \tag{3}$$

Where x is the color under encryption (R, G, B), z is the binary sequence used. The relation between x and z is shown in table (1). The relation between x and z will be altered after each swapping operation.

	z, x	*z, x*	*z, x*
Dr	0, R	2, G	1, B
NRP	1, R	0, G	2, B
XoR	2, R	1, G	0, B

Table 1 relation between x and z

3.3 Swapping Process of Binary Sequences

To generalize the encryption dependency of pixels colors on all used binary sequences, we used a procedure for binary sequences swapping. This procedure is initiated according to the following condition,

```
    If decimal value of $S_3(0\ldots11)$ mod decimal value of $S_3(4\ldots11)$ =0 then start swapping procedure.
  If $S_0(0)$=1 then interchange $S_0$ and $S_1$
  If $S_1(0)$=1 then interchange $S_1$ and $S_2$
  If $S_2(0)$=1 then interchange $S_2$ and $S_3$
  If $S_3(0)$=1 then interchange $S_3$ and $S_0$
```

After this sequence swapping procedure the role of S_0, S_1, S_2 and S_3 in the encryption process will be interchanged.

3.4 Grayscale Image Encryption

For grayscale image Encryption, in the original image we have R=G=B. we apply the same encryption procedure for color image, but in this case we will have R≠G≠B. we will pick randomly one value among R,G, and B to be the color of the pixel according to the following procedure.

```
Select case decimal value of $S_3(0\ldots11)$ mod 3
Case = 0: G = R,  B = R
Case = 1: R = G, B = G
Case = 2: R = B, G = B
End select
```

4. ENCRYPTION SYSTEM ANALYSIS AND SIMULATION RESULTS

To measure the strength of this encryption system against illegal decryption trials, we consider the following:
The FBG used for binary sequences generation, requires as initial condition around 13000 bits to start generation process of one sequence. This generator had proved its random behavior and had very good correlation properties [10]. To decrypt one pixel, we have to guess 48 bit with possible number of 2^{48}, to decrypt the whole image the number of guesses 2^{48*N*M}. so for an image of dimensions 256*256 we have $2^{3145728}$ possible encryption result.
Our system is four keys dependent, changing one key and preserving the other three in the decryption process will not reveal any useful data of the original image. This is shown in Fig. 3.
The encryption system is image content dependent, which provide an advantage in security level of our system.

In simulation, four images are used. We stated the results of one of them in Fig. 1, which represents the result of color encrypted image. Also we provided the histogram of the encrypted images, the fractal Analysis plot Fig. 2.
The most direct method to examine the disorderly degree of the encrypted image is by sense of sight. But to ensure the encryption quality of our system, we used the fractal dimension (*fd*) as quantitative measure [8]. Also we examined the histogram of the encrypted image, which appeared almost flat. We calculate the Chi-squared of this histogram to test its randomness. Table (2) contains these results.
The fractal dimensions of the encrypted images range from 2.9999 to 2.9997. Since the maximal fractal dimension for a 2-dimensional surface is 3.00, the encryption results of our encryption system are completely disorderly.
The chi-squared value for 255 degree of freedom has a limit of 292.84 for a significance level of 5% [9]. The value for encrypted images ranges from 267.42 to 261.92. This indicates the random appearance of the encrypted image.

Image / Measure	Autumn (Gray S.)	Flower (Gray S.)	Radiance (Gray S.)	Paradise (Colored)		
				Red	Green	Blue
fd original	2.80264	2.38148	2.481747	2.32103	2.34185	2.36543
fd encrypted	2.999901	2.99975	2.99987	2.99996	2.99994	2.99986
Chi-squared enc.	261.92	267.42	264.743	248.59	237.11	245.18

Table 2: *fd* and Histogram Survey

5. CONCLUSION

In this paper, a new image encryption system has been proposed. The system is used for color images, and can be easily adopted for gray-scale images. The simulation had proved that, the system provide high disorder appearance for the encrypted image, and high dependency on 4 sequences. The encryption system is image content dependent, which provide an advantage in the security level.

6. REFERENCES

[1] Menezes, P. van Oorschot, and S. anstone, Handbook of Applied Cryptography, CRC Press, 1996.

[2] W. Diffie and M. E. Hellman, “Privacy and authentication: an introduction to cryptography,” *Proceedings of the IEEE*, vol. 67, pp. 397-427, 1979.

[3] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, “Information Hiding - A Survey” *Proceedings of the IEEE*, special issue on protection of multimedia content, 87(7): 1062{1078, July 1999.

[4] Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom,” Watermarking Applications and Their Properties”, Int. Conf. on Information Technology’2000, Las Vegas, 2000

[5] Chen Hun-Chen, Yen Jui-Cheng, and Guo Jiun-In “Internet Security - Design of a New Cryptography System”, *Lecture Notes in Computer Science, 2002, pp*. 1041-1048

[6] Shujun Li and Xuan Zheng, “On the Security of an Image Encryption Method”, *IEEE Proceedings of ICIP 2002*, vol. 2, pp. 925-928

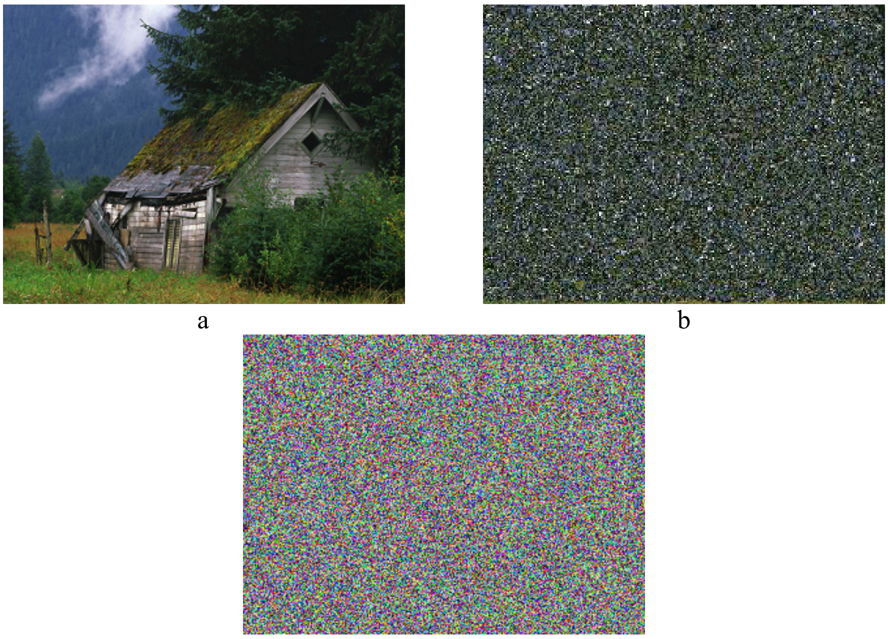
[7] Bruce Schneier, Applied Cryptography, Jhon Wiely & Sons, Inc., New York, 2nd edition, 1996

[8] C. Chen, J. S. Daponte, and M. D. Fox, “Fractal Feature Analysis and Classification In Medical Imaging”. *IEEE Trans. on Medical Imaging*, vol. 8, 1989, pp. 133-142.

[9] Catherine M. Thompson, Table of percentage points of X^2 distribution, Biometrika, Vol. 32, 1941.

[10] Said E. El- Khamy, Mona Lotfy, and Adel Hamdi Ali, “A New Fuzzy Logic Based Pseudo-Random Bit Generator for Secure DS-CDMA Systems”, 22nd URSI NRSC Conference, Cairo, Egypt, March 2005, C22.

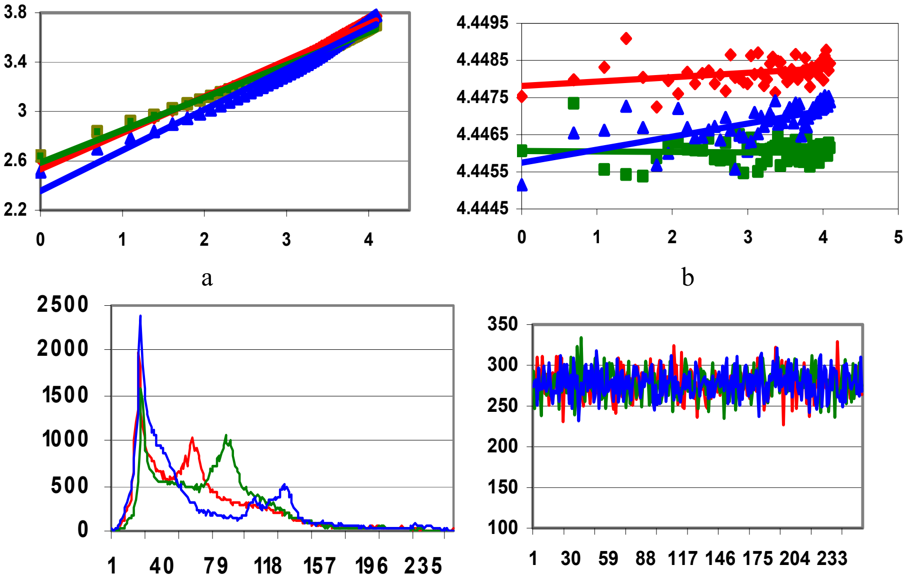
[11] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Addison-Wesley, 1992.



a b

c

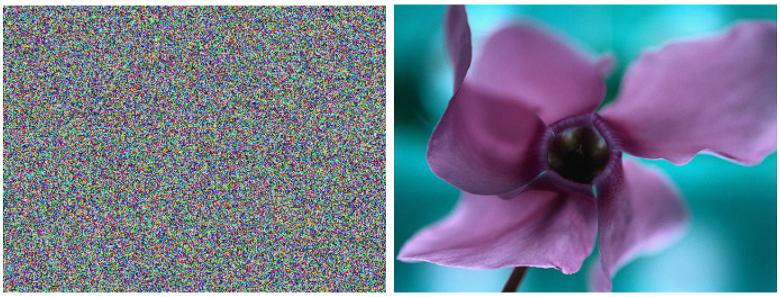
Fig. 1 "Shed in Field" image (a) original, (b) permuted, (c) encrypted.



a b

c d

Fig. 2 "Shed In Field" Image (a, b) Fractal Analysis of R, G, and B Colors Original & Encrypted Respectively. (c, d) Histogram of R, G, B Colors Original & Encrypted Respectively



a b

Fig. 3 “Flower” image (a) decrypted using 3 correct keys only, (b) original