New Method for Image Encryption Using GOST And Chaotic Tent Map

Amina Yahi[1*], Tewfik Bekkouche[2], and Nacira Diffellah[3]

[1]ETA Laboratory, Department of
Electronic, University of Bordj Bou
Arreridj 34030, Algeria
amina.yahi994@gmail.com

Abstract. This research paper proposes a simple and an efficient image encryption scheme based on chaotic tent map and GOST algorithm, which is the Russian norm of encryption. The tent chaotic system was used to generate chaotic random keys, as well as a chaotic shift values that used in the GOST algorithm, in order to provide security as a higher strength. The obtained simulation results prove the performances of the proposed method in term of histograms analysis data loss and sensitivity test.

Keywords: Encryption· Tent chaotic map· Image· GOST.

1 Introduction

Since 1990, communication networks created a revolution in the use of information; this information cannot be only a text but also audio, image, and so on. The protection of these informations must be provided, giving their sensibility and privacy of the major part of them, therefore the field of multimedia security was first motivated partly by the increasing use of digital means to communicate store and represent entertainment information such as music and video [1].
Encryption is one of the solutions used to protect our transmitted informations, it is the process of modulating data or information [2]. Chaos-based image encryption (IE) algorithms are more frequently used in the digital IE due to large data capacity and strong correlation among pixels [3].
Furthermore, GOST is a block cipher algorithm invented in Russia and based on the structure Feistel network encryption [4]. This algorithm is a simple and a clear encryption algorithm, it performs some processes (rounds), which are equal to 32 rounds (round), and uses 64-bit block cipher with a 256-bit key, the details of this technic are described in figure 1. The weak point of the algorithm GOST is a simple key schedule [5], this can be resolved by the use of chaotic key generators.
The main idea in this work is to mix between the GOST and a chaotic system, in order to provide an efficient encryption method. Experimental results using Matlab environmental prove the efficiency of the proposed scheme.
The remainder of this paper is organized as follows: in section 2, we explained both the proposed encryption and decryption schemes, in section 3; we showed simulation results and security analysis, and finally some concluding remarks are given in section 4.

2 Encryption/Decryption Method

2.1 Tent Chaotic Map

It was used by many researchers in cryptography, because of their high sensitivity to their initial values and control parameters [7], in this proposed method, it was used the tent chaotic map, which is defined as follows [8]:

$$x_{n+1} = T(r, x_n) := \begin{cases} rx_n & when\ x_n < 0.5 \\ r(1 - x_n) & otherwise \end{cases} \quad (1)$$

Where $x_n$is the vector stat, and r is the control parameter. It has robust chaos for control parameter $r = 2$ [9].

2.2 Encryption Scheme

The following steps describe the proposed encryption algorithm process:

a) First step of encryption

Let P be the original image in greyscale of size$(N \times N)$, and BN be the chosen blocs number per line. First, we generate a chaotic vector of size BN, using the tent map. Then we divide P into BN rows and BN columns. So we obtain $(BN \times BN)$ smaller sub-images (or blocs) of size $(m \times m)$, with $m = N/BN$, in order to reorder each row and each column blocs according to the previous generated random chaotic vector as illustrated in figure 2.

b) Second step of encryption

Here, we generate the rest of keys chaotically that will be used in the modified GOST algorithm. First, we will use the sequences generated from tent map in three locations, for three reasons:

- To generate the binary vector key of 32 bit and $32 \times BN \times BN$ colomn (as shown in figure 3).
- To generate a chaotic S-box matrix$(32 \times BN \times BN)$.
- To generate the cyclic shift matrix (CSM) of $(32 \times BN.BN)$, the values of CSM vary between 1 and 11, and it is obtained by using the following expression:

$$CS(i) = 10 \times x(i) \quad (2)$$

c) The third step of encryption

Reshape each bloc from the image into $\left(\frac{m.m}{8} \times 8\right)$, and convert each pixel from the new bloc to 8 bits, after that we will have 64 bit in each line of each bloc. As shown in Figure 3, the right side of the first sub bloc is followed by a function F, which converts the sub bloc into three cryptographic processes: data addition and our first generated key module 2^{32}, data substitution using S-boxes, in this case we performs the bitxor operation between the left side and the output of the s-box, then the cyclic left shift to x positions according to the value of cyclic shift matrix(CSM). The output of F is added to the left side. The next round is swapped on the right and left sides. There are 32 rounds in the algorithm. Unlike, right and left sections are not changed during the last encryption cycle.

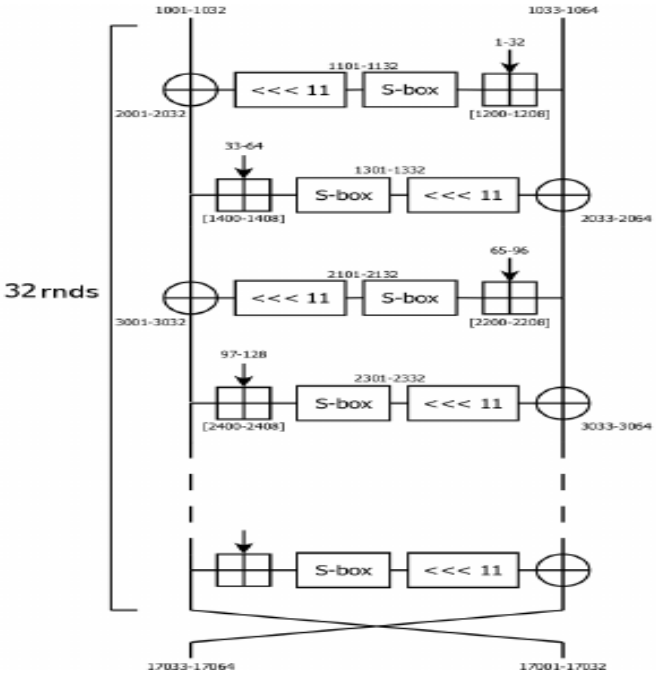

Fig. 1. Scheme of bloc cipher GOST.

2.3 Decryption Scheme

The process taken in this stage is the same with the encryption process in inverse manner.

3 Simulations Results and Security Analysis

3.1 Histogram Analysis

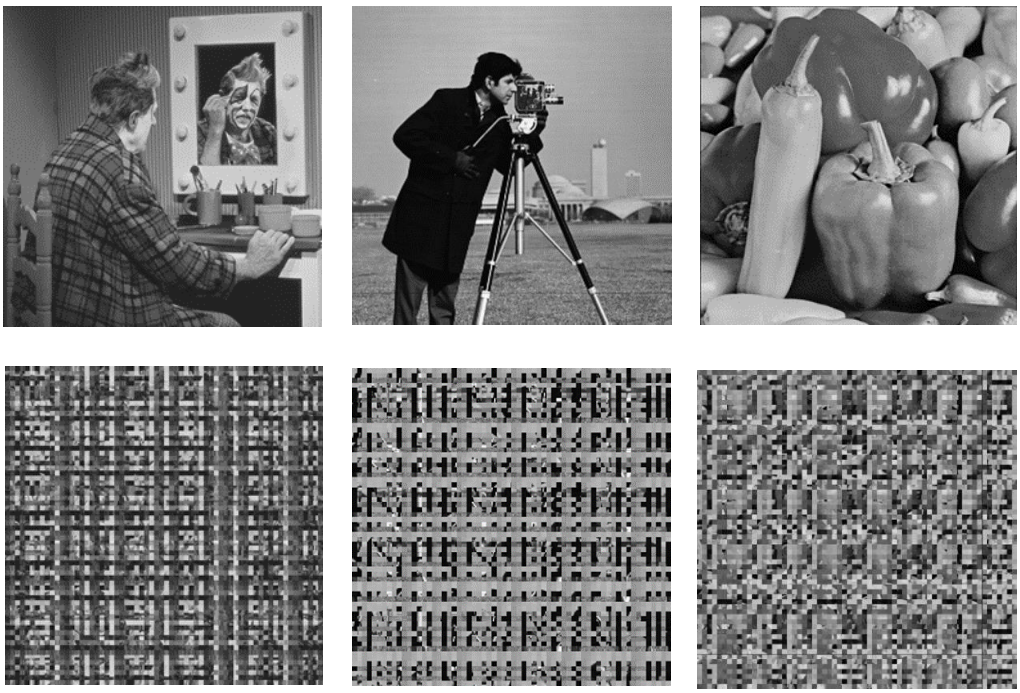

Fig. 2. Peppers, Cameraman, Clown, and their scrambled versions.

We note that the histogram of the encrypted image look like uniform, where all pixel values have the same probability of occurring, by analyzing histogram we conclude that this approach resists attacks.

3.2 Entropy Analysis

For grayscale image encryption, the value of the entropy must be very close to 8 [10], his formula is expressed below:

$$H(s) = \sum_{i=1}^{2^N-1} P(s_i) log \frac{1}{P(s_i)} \quad (3)$$

Where $P(s_i)$ represents the probability of the appearance of pixels in the image. According to Table. 1. It is seen that the obtained entropy numbers by this algorithm are quite close to the theoretical value of 8. Thus, the proposed method have better chaotic distribution.

Table 1. Entropy values.

Encrypted images	Entropy
Peppers	7.9992
Barbara	7.9972
Cameraman	7.9970
Clown	7.9993

3.3 Data Loss

During Digital images transmission, it can be occur different phenomena as data loss

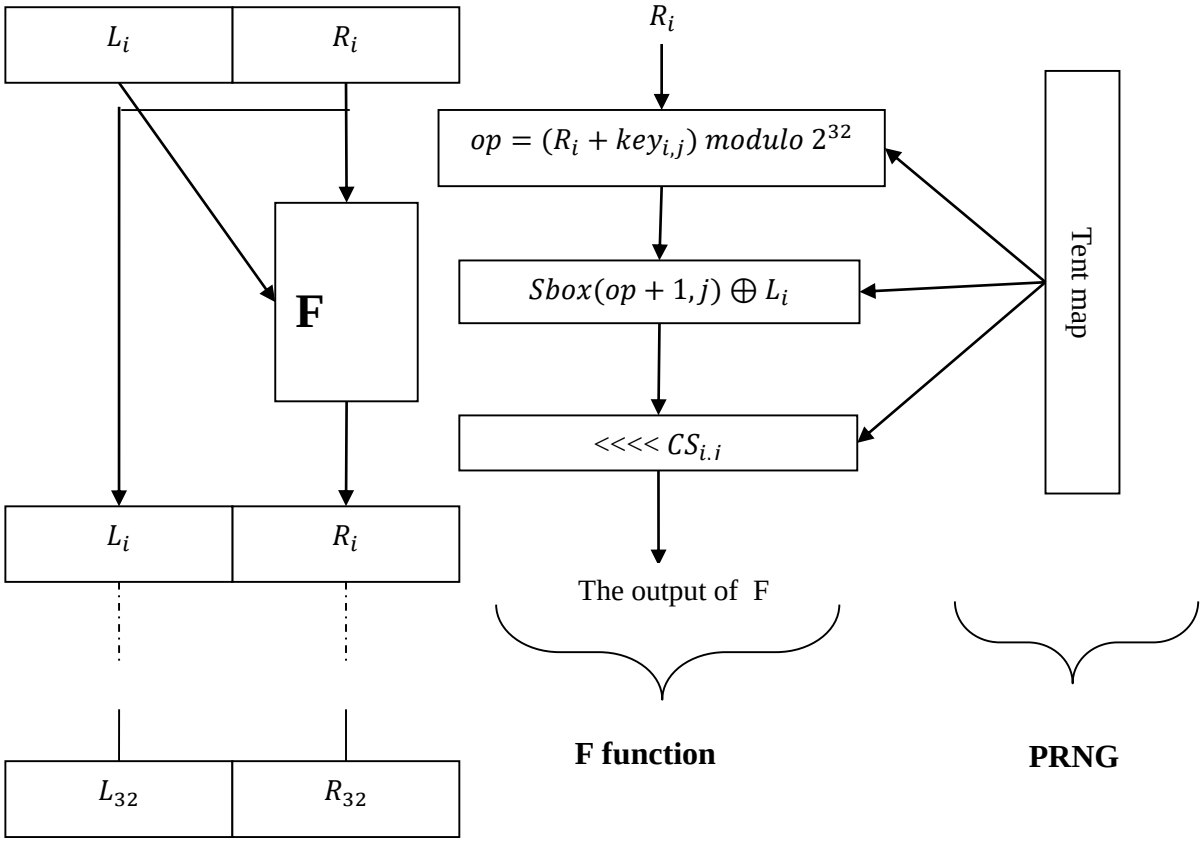

Fig. 3. Block diagram of the modified GOST.

through the network and during storage. A good image encryption algorithm should resist these abnormal phenomena. The use of data loss on the encrypted image is to verify the ability of resistance to attack. The cameraman image is encrypted by the presented algorithm, then on this encrypted image is applied a data loss with a size of 128×128 (Fig. 5a), 128×128 in the middle (Fig. 5b), and 128×256 (Fig. 5c). The proposed scheme is robust against data loss, because their decrypted images shown in Figs. 5a, b and c contain majority of original visual information.

3.4 Key Sensitivity Analysis

To observe the effect of the key on the decrypted image. Each key is changed by 10^{-15} Fig. 6a illustrates the decrypted cameraman image when the value of the control parameter is changed by 10^{-15}. In Fig. 6b, c, d, and e, we have the decrypted image of cameraman image when the initial values is changed by 10^{-15}. Hence, a tiny change in the key can damage the decrypted image, And from it we conclude that our image encryption scheme is extremely sensitive to its key.

3.5 Correlation Coefficients

It is used to calculate the correlation between two pixels in the horizontal, vertical, and diagonal directions in the original image and encrypted image. Fig. 5. Shows respectively the correlation distributions of the horizontal, vertical and diagonal adjacent pixels of the original image and the encrypted image.

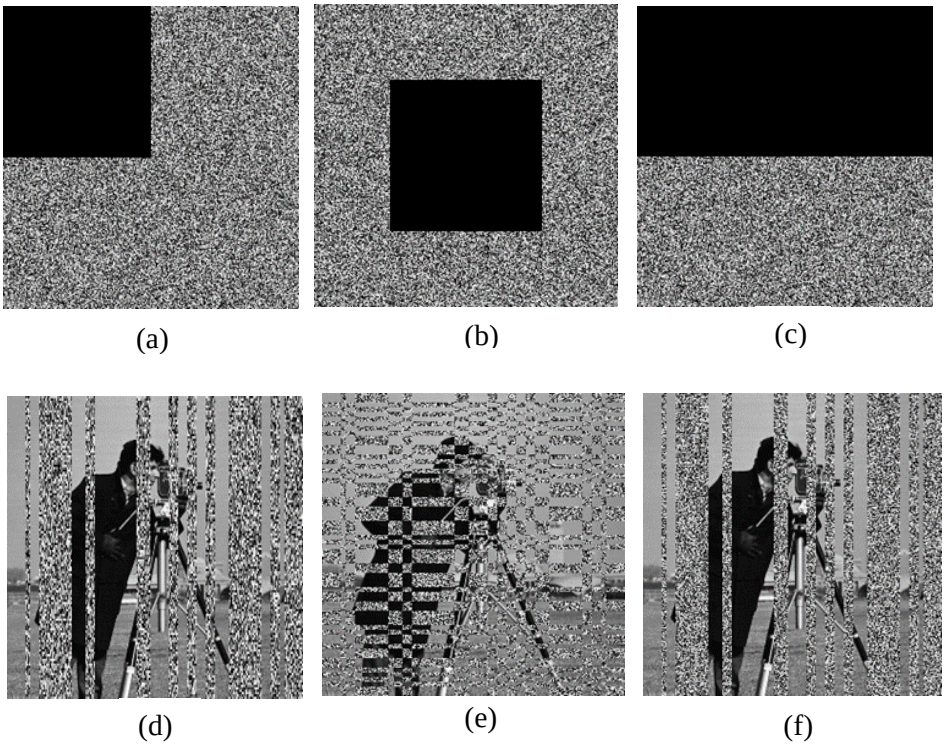

Fig. 5. Data loss. (a) Encrypted image with 128×128 data loss. (b) Decrypted image of a. (b) Encrypted image with 128×128 data loss in the middle. (c) Encrypted image with 128×256 data loss. (d) Decrypted image of (a). (e) Decrypted image of (b). (f) Decrypted image of (c).

3.6 Key Space Security

For efficient security the key space must be $> 2^{100}$ [11], let's admit that the key's precision is 10^{-15}. In our encryption scheme, we have the following set of keys:

- The key of the first step (x_1, r).
- The key of the second step$((x_2, r), (x_3, r), (x_4, r))$.

So the total key is $10^{15\times5}$, which explain that it's great for opposing a brute force attack.

4 Conclusion

This article introduced a new image for encrypting digital grey scale images, using chaotic tent map and GOST, first we perform a bloc image shuffling using jigsaw permutation using tent map, and then we apply a modified GOST encryption technique on the resulting image. The results given by this study are up to the other works not only that, but also this algorithm is one of the new method of image encryption, at our knowledge.

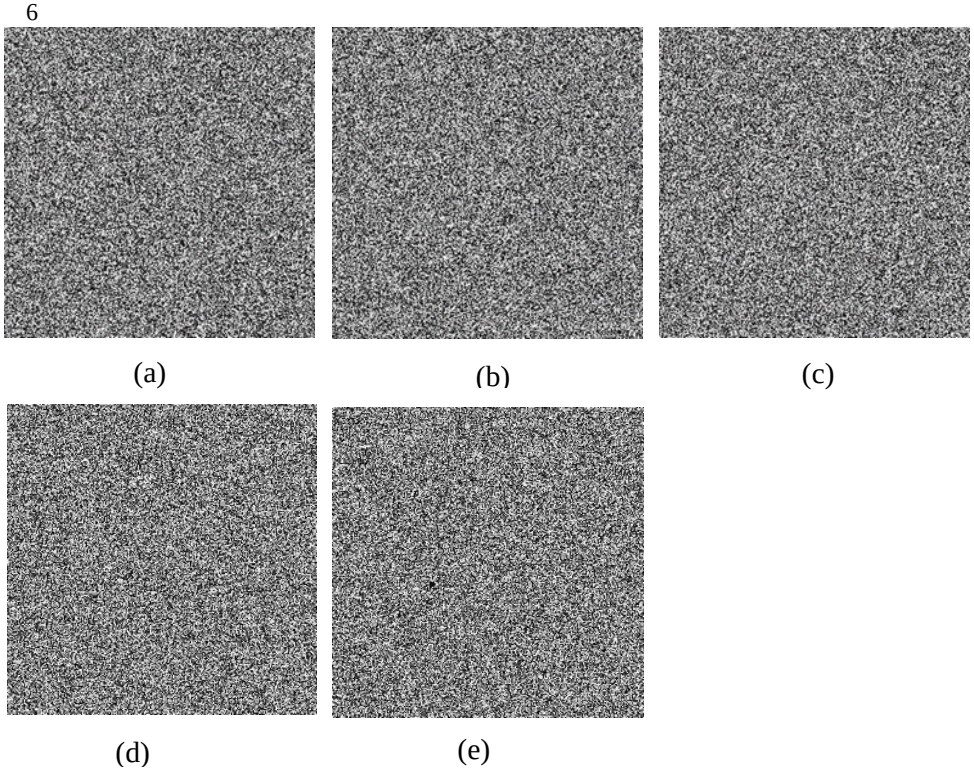

Fig. 6. Decryption image with small changing in key. (a) Decrypted image with $r + 10^{-15}$. (b) Decrypted image with $x_1 + 10^{-15}$. (c) Decrypted image with $x_2 + 10^{-15}$.(d) Decrypted image with $x_3 + 10^{-15}$. (e) Decrypted image with $x_4 + 10^{-15}$.

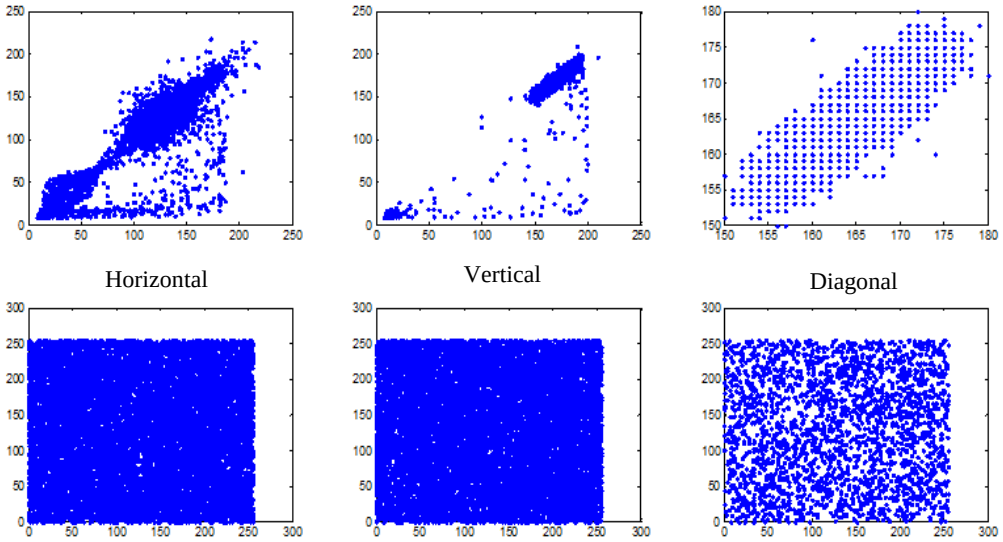

Fig. 7. The correlation analysis on Cameraman image and its encrypted image by the proposed algorithm

References

1. Abd El-Samie FE and Al (2014) IMAGE ENCRYPTION: A Communication perspective. Taylor & Francis Group, LLC
2. Sathish Kumar GA, Bhoopathy K, Sriramet N, and Al (2011) Image encryption based on diffusion and multiple. Int. J. Network Secur. vol 3, pp 181-194.
3. Yousif B and Al (2020) A novel image encryption scheme based on integrating multiple chaotic map. AIP Advances 10.
4. Iqbal M, Siahaan APU (2016)The understanding of GOST Cryptography Technique. International Journal of Engineering Trends and Technology. vol. 39, pp 168-172.
5. Najm H, Hoomod HK (2021) A New Wot Cryptography Algorithm based on GOST and a Novel 5d Chaotic System. iJIM, vol. 15, no. 2.
6. Zajac P, Čagala R (2012) Local reduction and the algebraic cryptanalysis of the block cipher gost. : Periodica Mathematica Hungarica, vol 65, no 2, pp 239-255.
7. Pak C,Huang L (2017)A new color image encryption using combination of the 1D chaotic map : Signal processing. vol 138, pp 129-137.
8. Kanso A (2011) Self-shrinking chaotic stream ciphers. Commun. Nonlinear Sci. Numer. Simul. 16(2), 822–836.
9. Khan MA, and Al (2014) Modified chaotic tent map with improved robust region. IEEE 11-th Malaysia International Conference on Communications (MICC), 2014.
10. Shafique A, Shahid J (2018) Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. The European Physical Journal Plus, vol. 133, no. 331, pp 822-836.
11. Wang X, Wang S, Zhang Y and al (2017) A novel image encryption algorithm based on chaotic shuffling method. Inf. Secur J, Glob. Perspect. Vol 26(1), pp 7–16