A Stream Cipher Algorithm based on Nonlinear Combination Generator with Enhanced Security for Image Encryption

Aissa Belmeguenai
Laboratoire de Recherche en Electronique de Skikda – Université du 20 août 1955 Skikda – 21000 Algeria

Mohammed Redjimi
Department of computer science – University of 20 August 1955- Skikda 21000 Algeria

Nadir Derouiche
Laboratoire de Recherche en Electronique de Skikda – Université du 20 août 1955 Skikda – 21000 Algeria

ABSTRACT

This paper describes a novel approach for image encryption using stream cipher algorithm based on non linear combination generator. This work aims to enhance the security of encrypted image. The work is based on the use of several linear feedback shifts registers whose feedback polynomials are primitive and of degrees are all pair wise cop rimes combined by resilient function whose resiliency order, algebraic degree and nonlinearity attain Siegenthaler's, Sarkar and al.'s bounds. This proposed approach is simple and highly efficient. The proposed algorithm was evaluated through a set of tests. In order to have a global idea of the whole performance of system, our tests included visual tests, histogram analysis, key space analysis, Berlkamp-Massey attack, correlation attack and algebraic attack. The results of the experimental tests demonstrate that the proposed system is highly key sensitive, highly resistant to noises and shows a good resistance against brute-force, statistical attacks, Berlekamp-Massey attack, correlation attack and algebraic attack. The system is robust which makes it a potential candidate for image encryption.

General Terms

Cryptography system

Keywords

Cryptosystem, Image correlation, Image encryption and decryption, Key stream, Non linear combination generator resilient function, LSFR

1. INTRODUCTION

We assist today to an explosion of numerical networks. These networks vehicle a big quantity of information and are inter-connected and connected to internet. The information circulates freely in several forms: textual, audio, digital images and other and can be intercepted by persons and systems for whom they are not intended and can be, therefore, diverted, copied, falsified, exchanged, stored... The problem is even graver if it is about confidential or vital information such are the cases of the medical information, the industrial and military secret, bank secret accounts, etc. It is, thus necessary to protect them from any undesirable interception by making them incomprehensible for all intruded systems. The modern cipher of data is effective means to resolve this problem.

This paper presents a cipher system for data image security. Data images have specific particularities because of their information which is two-dimensional and redundant nature and request bigger capacities. An image of n lines and m columns is composed of nxm pixels and requests kxnxm bits if each pixel is coded on k bits. For example; an image of 1024x1024 pixels requests a space memory of (3x8)x1024x1024 = 24 Mbits if each pixel is coded on one byte. Therefore, the classical cryptographic algorithms such as RSA, DES, etc. are inefficient for image encryption due to image inherent features in particular regarding of high volume image data. Different image encryption schemes was proposed in this domain [1][2][3][4]. The proposed encryption scheme is a simple, fast and secure approach for image encryption using a stream cipher algorithm which combines several linear feedback shift registers (LSFRs) by Boolean functions satisfying all criteria cryptographic for maximum safety. This algorithm is robust and very sensitive to small changes in key so even with the knowledge of the approximate key value.

2. STREAM CIPHER BASED ON NON LINEAR COMBINATION GENERATORS

Generally, stream ciphers are based on linear feedback shift registers (LSFRs). An LSFR of length L is a L stage register with a linear feedback function. During its operation, contents of each storage unit are shifted to the next unit and the output of the feedback function is fed to the last storage unit. If the feedback function of the LFSR is primitive and its initial state is a non-zero state, then the output sequence produced by the LFSR has the maximum period of $2^L -1$.

A system of stream cipher based on nonlinear combination generator, generally, breaks up into three parts: An engine, primarily made up of linear feedback shift register with maximum period, the goal of this engine is to provide one or more continuations, having good statistical properties. Already; generally, registers (LFSRs) are used whose feedback polynomials are primitives and of degrees are all pair wise cop rimes.

The outputs of the (LFSRs), having more or less strong properties of linearity, it is essential to make disappear to the maximum these properties of linearity. The second part is thus a module whose role is to break this linearity by combining the outputs to (LFSRs) by a nonlinear Boolean function having the best possible cryptographic properties. These a nonlinear Boolean function must be selected very carefully to offer a resistance to the attacks.

A module of combination the key stream with the plaintext, most common is reduced to a modulo2 addition (XOR). The key stream $(z_t)_{t\geq 0}$ is generated as a nonlinear function f of the outputs of the component LFSRs. Such key stream generator is called nonlinear combination generator, and f is called the combining function. The outputs of f is bitwise XORed with the plaintext $(m_t)_{t\geq 0}$ to produce the cipher text $(c_t)_{t\geq 0}$, this construction is illustrated in figure 1.

The combining function must have high algebraic degree, high nonlinearity and good correlation immunity to prevent correlation and linear attacks [5, 6, 7, 8]. It must also have high algebraic immunity to provide resistance against the algebraic attacks. [9] [10] [11] [12] [13] [14].

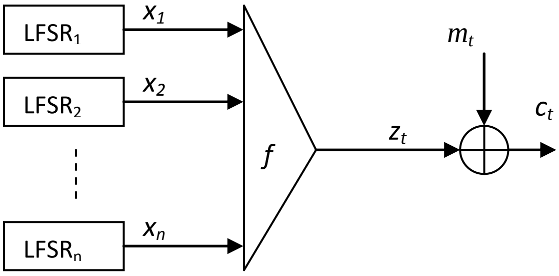

Fig. 1. System of Stream Cipher Based on Nonlinear Combination Generator

3. PROPOSED APPROACH

The approach used stream ciphers algorithm based on nonlinear combination generator for constructing our new approach. The layout of our method is presented in Figure 2. Let *13* LFSRs denoted $R_1, R_2, ..., R_{13}$ whose respectively length $L_1, L_2, ..., L_{13}$ are pairwise distinct greater than 2, are combined by a nonlinear function f as in figure 1 which is expressed in algebraic normal form. Denote the output of R_i at time t by $s_i(t)$. Then the key stream $z(t)$ is given as

$$z(t) = f\left(s_1(t), s_2(t), ..., s_{13}(t)\right) \quad (1)$$

The linear complexity of the key stream is $\lambda(s) = f\left(L_1, L_2, ..., L_{13}\right)$ is evaluated over the integers rather than over Z_2.

Let Y an original image (plain-image) of $n \times m$ pixels. First, sender transforms the plain image Y into binary array (plain image digit). Let $y(t), c(t)$ and $z(t)$ be the plain image digit, cipher image digit and key stream digit at time t. Then the encryption process can be described by the equation

$$c(t) = y(t) \oplus z(t) \quad (2)$$

where $\oplus$ is the function XOR (Or exclusive). The cipher image digit $c(t)$ is sent to the receiver over an unsecure channel and is decrypted a bitwise XOR operation the key stream digit and the plaint image digit can be described as

$$y(t) = c(t) \oplus z(t) \quad (3)$$

The cipher image digit at the receiver is decrypted by producing the same key stream. The receiver transforms the decrypt image digit in to plain image y of $n \times m$ pixels. Their main advantages are their extreme speeds and their capacity to change every symbol of the plaintext. Besides, they are thus used in a privileged way in the case of communications likely to be strongly disturbed because they have the advantage of not propagating the errors [15].

3.1 Key K

The secret key K of the cryptosystem is then either made up of the initialization of only one register but of 13 registers is a chain of bits length

$$53+59+61+67+71+73+79+83+89+91+95+101+102=1024$$

bits. This chain of bits must be sufficiently large in order to guarantee a maximum security and also to avoid, at the present time and with reasonable means, any attempt at against brute-force attack.

3.2 LFSRs

We considered thirteen maximum-length LFSRs whose lengths L_i , $i \in [1,...,13]$ are all pairwise coprimes which feedback polynomials are respectively $p_1, ..., p_{13}$. We chose the following feedback polynomials:

$$p_1(x) = x^{53} + x^6 + x^2 + x + 1,$$
$$p_2(x) = x^{59} + x^{22} + x^{21} + x + 1,$$

$$p_3(x) = x^{61} + x^5 + x^2 + x + 1,$$
$$p_4(x) = x^{67} + x^5 + x^2 + x + 1,$$

$$p_5(x) = x^{71} + x^5 + x^3 + x + 1,$$
$$p_6(x) = x^{73} + x^4 + x^3 + x^2 + 1,$$

$$p_7(x) = x^{79} + x^4 + x^3 + x^2 + 1,$$
$$p_8(x) = x^{83} + x^7 + x^4 + x^2 + 1 ,$$

$$p_9(x) = x^{89} + x^6 + x^5 + x^3 + 1,$$
$$p_{10}(x) = x^{91} + x^7 + x^6 + x^5 + x^3 + x^2 + 1,$$
$$p_{11}(x) = x^{95} + x^6 + x^5 + x^4 + x^2 + x + 1,$$
$$p_{12}(x) = x^{101} + x^7 + x^6 + x + 1$$

$$p_{13}(x) = x^{102} + x^6 + x^5 + x^3 + 1.$$

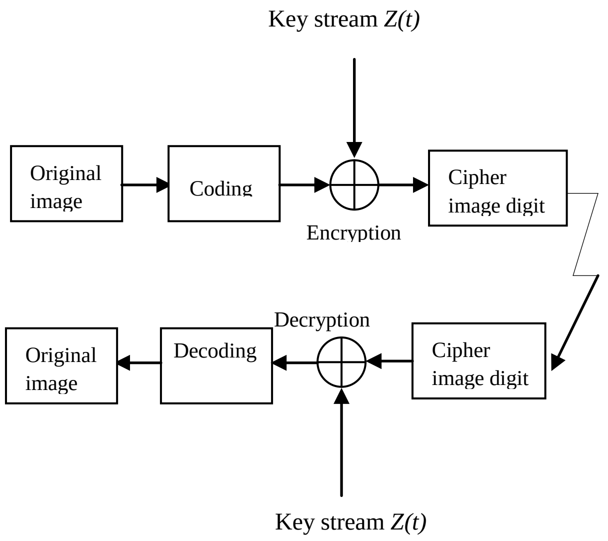

Fig. 2. Block Diagram of the Proposed Approach;

3.3 Nonlinear Combining Function

The combining function used for generating the key stream is a Boolean function f from F_2^{13} into F_2. At each time t, thirteen sequences bits $s_1(t), s_2(t),..., s_{13}(t)$ are inputs to the Boolean function f to calculate the key stream $z(t)$ as show equation (1).

The combining function f used in our approach is presented in [16]. This function is 5-resilient function, of algebraic degree 7 and nonlinearity $Nf = 3969$ with algebraic immunity 6, satisfies all the cryptographic criteria necessary carrying out the best possible compromises.

3.4 Algorithm1: Encryption and Decryption Image Algorithm

3.4.1 Encryption

```
- Load the plain-image $Y$ (i.e. Original image);
- Transform the plain-image into column digit (i.e. plain image digit) and to store them in $y$ ;
- $N \leftarrow$ the length of $y$ ;
- for $t = 1$ to $N$ to make ;
- To generate the key-stream $z(t) = f(s_1(t), s_2(t),..., s_n(t))$ as show the algorithm 2 ;
- End to make ;
- for $t = 1$ to $N$ to make
- Calculate the cipher image digit using relation $c(t) = XOR(y(t), z(t))$ ;
- End to make ;
- Sent the cipher image digit.
```

3.4.2 Decryption

```
- Load the cipher-image digit $c$
- $N \leftarrow$ the length of $c$ ;
- for $t = 1$ to $N$ to make ;
- To generate the key stream $z(t) = f(s_1(t), s_2(t),..., s_{13}(t))$ as show the algorithm 2;
- End to make ;
- for $t = 1$ to $N$ to make;
- Calculate the decipher image digit using relation $y(t) = xor(c(t), z(t))$ ;
- End to make ;
- To put the decipher image digit $y$ in the form of an image of $n \times m$ pixels and to store it in $Y$ ;
```

3.5 Algorithm2: Key stream

```
- To read $N$ , length of $y$ ;
- To introduce the secret key, the value of initialization of 13 registers ;
- for $t = 1$ to $N$ to make;
- To generate the output of $s_1(t), s_2(t),..., s_{13}(t)$ ;
- End to make ;
- for $t = 1$ to $N$ to make;
- To generate the key stream $z(t) = f(s_1(t), s_2(t),..., s_{13}(t))$;
- End to make.
```

4. TESTS RESULTS

In this section, the performance of the proposed image encryption scheme is analyzed in detail. We discuss the security analysis of the proposed image encryption scheme including some important ones like statistical sensitivity, key sensitivity analysis, key space analysis etc. to prove the proposed cryptosystem is secure against the most common attacks.

4.1 Visual Testing

A number of images are encrypted and decrypted by the proposed method, and visual test is performed. Two examples are shown in Fig. 3 (a) and Fig. 3 (d), with respectively 128 x 128 and 256x256 pixels. By comparing the original and the encrypted images in Fig. 3, there is no visual information observed in the encrypted image.

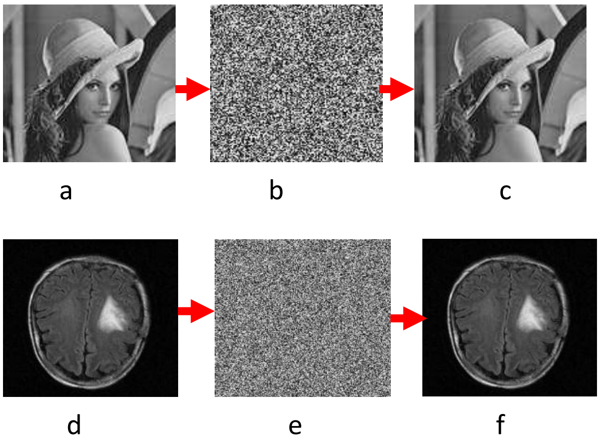

Fig. 3. Frame (a) and (d) Gray image show the original image of Lena and IRM, frame (b) and (e) respectively show the encrypted image, frame (c) and (f) respectively show the decrypted image.

Fig. 4, Frame (a) show the difference between original image figure 3(a) and decrypted image figure 3(c). Frame (b) show the difference between original image figure 3(d) and decrypted image figure 3(f).

Difference between original images and their decrypted images shown in figure 3, are illustrated in figure 4(a), 4(b), are prove that, there is no loss of information, the difference is always 0.

5. SECURITY ANALYSIS

5.1 Key Space Analysis

The key space should be large enough to make the exhaustive search attack infeasible. Since the algorithm has a chain of 1024bits is the initialization of 13 registers, the intruder needs 2^{1024} tests by exhaustive search. An image cipher with such as a long key space is sufficient for reliable practical use.

5.2 Histogram Analysis

In the experiments, the original images and its corresponding encrypted images are shown in figure 3, and their histograms are shown in figure 5. It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the histogram of the original image. So, the encrypted image does not provide any clue to employ any statistical attack on the proposed encryption of an image procedure, which makes statistical attacks difficult.

These properties tell that the proposed image encryption has high security against statistical attacks. In the original image (i.e. plain image), some gray-scale values in the range [0, 255] are still not existed, but every gray-scale values in the range [0, 255] are existed and uniformly distributed in the encrypted image. Some gray-scale values are still not existed in the encrypted image although the existed gray-scale values are uniformly distributed. Different images have been tested by the proposed image encryption procedure.

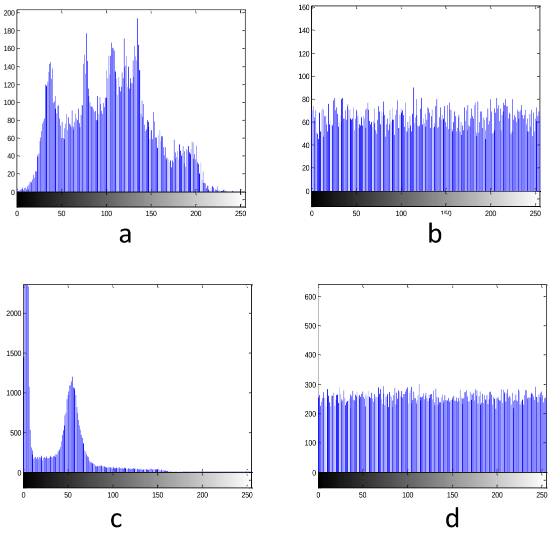

Fig. 5, Histogram analysis: Frame (a) and (c) respectively, show the histogram of the plain images shown in figure 3(a) and 3(d). Frame (b) and (d) respectively; show the histogram of the encrypted images shown in figure 3(b) and 3(f).

5.3 Correlation Coefficient Analysis

Correlation is a measure of the relationship between two variables. If the two variables are the original image and their encryptions then they are in prefect in correlation. In this case the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image**.** If the correlation coefficient equals zero, then the original image and its encryption are totally different i.e. the encryption image has no features and highly independent on the original image. If the correlation coefficient equal -1, this means encrypted image is a negative of the original image.

Table 1 gives the corresponding correlation coefficient between plain-images (i.e. original image) shown in figure 3(a), 3(d) and 6(a) and their encrypted images. It is observed that the correlation coefficient is a small correlation between plain-images and encrypted image.

Table 1. Correlation Coefficients analysis

Cases	**Correlation coefficient**
Image 3.a	-0.0086
Image 3.d	-0.0068
Image 6.a	-0,0055

5.4 Image Entropy

A secure cryptosystem should fulfill a condition on the information entropy that is the ciphered image should not provide any information about the plain image. It is well known that the entropy $E(m)$ of a message source m can be calculated as:

$$E(m)=\sum_{i=0}^{G-1} p(m_i)\log_2 \frac{1}{p(m_i)} \qquad (4)$$

Where G is the gray value of an input image (0-255), $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $m=\{m_1,m_2,...,m_{2^8}\}$. Truly random source entropy is equal to 8. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Table 2 gives the entropy values of plain images and of their encryptions images shown in figure 3 and 6. The values obtained are very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

Table 2. Image Entropy

Plain-Image	**Entropy**	**Encrypted Image**	**Entropy**
Image 3.a	7.4697	Image 3.b	7.9870
Image 3.d	5.4753	Image 3.e	7.9971
Image 6.a	2.8284	Image 6.c	7.9889

5.5 Key sensitivity analysis

An ideal image encryption procedure should be sensitive with respect to secret key. The change of a single bit in the secret key should produce a completely different encrypted image. To prove the robustness of the proposed scheme, sensitivity analysis with respect to key is performed. High key sensitivity is required by secure image cryptosystems, which means the cipher image cannot be decrypted correctly even if there is only a small difference between the encryption and decryption keys. In the key sensitivity tests, we change one bit of the key. Figure 6 show key sensitivity test result. It can be observed that the decryption with a slightly different key (different secret key or initial values) fails completely. Therefore, the proposed image encryption scheme is highly key sensitive.

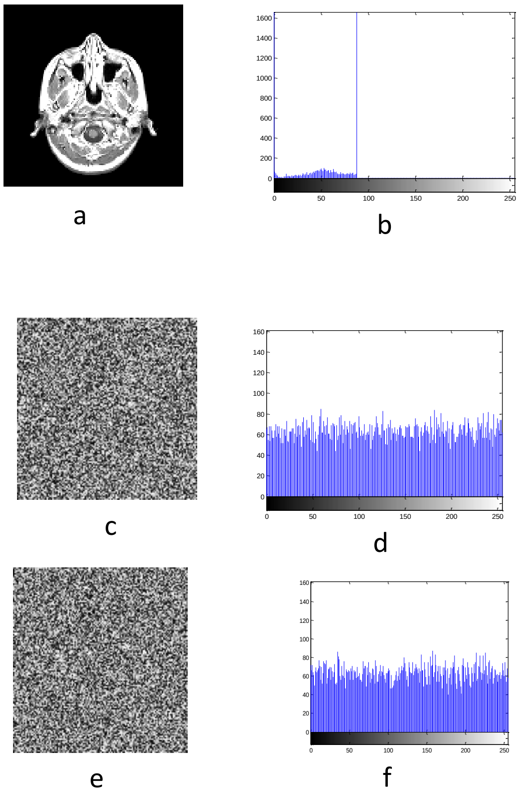

Fig. 6, Sensitivity analysis: (a) original mage of mri, (b) histogram of mri (c) encrypted image by a 1024 bits key, (d) histogram of encrypted image by a 1024 bits key, (e) decrypted image by key in (b) with a bit changed,(f) histogram of decrypted image by key in (b) with a bit changed.

5.6 Noise analysis

We also tested the resistance our cryptosystem to the noise by adding to the cipher-images a noise. From the cipher-images illustrated in the figures 3.b, and 3.e we added a noise of the same size of plain-images. The results are given in the figure 7a and 7.c. From the images 7a and 7.c, we apply the decryption algorithm presented in section 3.4; we have the results illustrated in figure 7b and 7.d. The noise added to ciphers-images 3.b, and 3.e is a matrix containing pseudo-random values drawn from a normal distribution with mean zero and standard deviation one, generates with function "randn". In this case examined, we can note that the decrypted images presented in figures 7b and 7.d are identical to the original images (see 3.a, 3.d), there is no difference pixel with pixel has indeed between the decrypted images and plain-images because of reversibility of our technique of encryption.

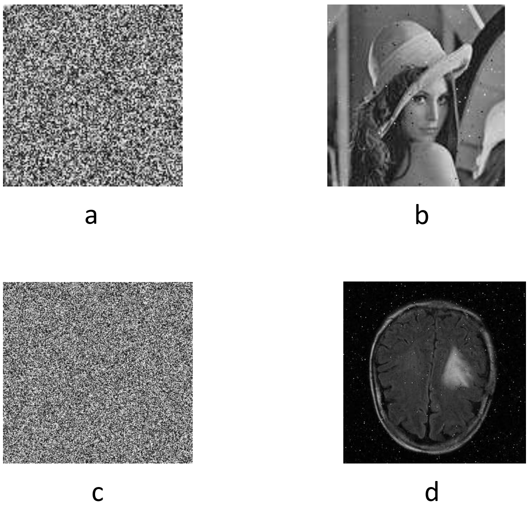

Fig. 7, Noise Analysis: Frame (a) show cipher image shown in figure 3 (b) with noise added , Frame (b) show deciphered image, Frame (c) show cipher image shown in figure 3 (e) with noise added , Frame (d) show deciphered image.

5.7 Berlekamps-Massey attack

The Berlekamps-Massey attack [17] requires $2\lambda(s)$ data successive. In order to mount a Berlekamp-Massey attack, the key stream generator must produces a key stream with linear complexity highest possible. This linear complexity depends entirely on the combining function. Linear complexity $\lambda(s) = f(53,59,...,101,102)$ used in our cryptosystem is between 2^{47} and 2^{48}, it is sufficiently large. This complexity completely excludes to use the Berlekamp-Massey attack.

5.8 Correlation Attack

The combining function f used in our system is correlation immune of order 5. In order to mount a correlation attack of Sigenthaler [18], the attacker must consider at least six shift registers simultaneously. The sum of the lengths of the shortest six LFSRs of the keystream generator is 53+59+61+67+71+73=384. Therefore, the complexity of Siegenthaler's correlation attack against our approach is at least $O(2^{384})$. This is out of reach this type of attack.

5.9 Algebraic Attack

In the algebraic attacks, the system is rewritten in the form of a nonlinear system of equations between the output of the filtering function f and its inputs in the following way:

$$z_0 = f(K) \;;$$

$$z_1 = f(h(K)) \;;$$

… ;

$$z_i = f(h^i(K)),$$

Here h denotes the linear update function to the next state of the LFSR's involved, K the total key of the system. Complexity to solve this system of equations strongly depends on the degree of these equations. The complexity $C(L,d)$ of the algebraic attack on the stream cipher system with a key of size L bits and equations of d degree is given by $C(L,d) = \left(\sum_{i=0}^{d}\binom{L}{i}\right)^{w} = L^{w.d}$, where w corresponds to the coefficient of the method of the solution most effective by the linear system and d is equal to algebraic immunity of the function of combination. We employ here the expression of Strassen [19] which is $w = \log_2(7) \approx 2.807$. In proposed cryptosystem the secret key is 1024 bits and the algebraic immunity of the nonlinear filter function is equal to 6. This leads to an algebraic attack with a complexity which is between 2^{168} and 2^{169}, which is sufficiently large. It is not easy to make a linear approximation of the nonlinear filter function within the framework of an algebraic attack.

6. CONCLUSION

In this paper, an encryption scheme using stream cipher based on nonlinear combination generator presented. The proposed encryption system included two major parts, 13 LFSRS with maximum period whose length are all pairwise comprimes, the goal of this engine is to provide one or more continuations, having good statistical properties already and nonlinear Boolean function satisfying all the cryptographic criteria necessary carrying out the best possible compromises. Simulations were carried out different images. The encrypted images obtained for these input images and the corresponding histograms are discussed. It is seen that encrypted images does not have residuals information and the corresponding histograms are almost flat offering good security for images. The proposed schemes key space is large enough to resist all kinds of brute-force attack. In addition, this method is very simple to implement, the encryption and decryption of image. Here the security aspects like key space, statistical and sensitivity with respect to key are discussed with examples. It is seen that the present cryptosystem is secure against the statistical, brute force and cryptanalytic attacks.

7. REFERENCES

[1] Sharma, M. and Kowar, M. K. 2010 ' Image Encryption Techniques Using Chaotic Schemes: a Review', International Journal of Engineering Science and Technology, vol. 2, no. 6, pp. 2359–2363.

[2] Jolfaei, A. and Mirghadri, A. 2010 'An Applied Imagery Encryption Algorithm Based on Shuffling and Baker's Map' Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR-10), Florida, USA,, pp. 279–285.

[3] Jolfaei, A. and Mirghadri, A. 2010 ‘A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1’, Proceedings of The 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10), Sanya, China.

[4] Xiangdong, L., Junxing, Z,. Jinhai, Z. and Xiqin, H. 2008 ‘Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation’ IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 1, pp. 64–68.

[5] Siegenthaler, T. January 1985 ‘ Decrypting a class of stream ciphers using cipher text only’, IEEE Transactions on Computers, C-34(1):81–85.

[6] Canteaut A. and Trabbia, M. 2000 ‘Improved fast correlation attacks using parity-check equations of weight 4 and 5’, Advanced in Cryptology-EUROCRYPT 2000. Lecture notes in computer science 1807 , pp. 573-588.

[7] Johansson, T. and Jonsson, F. 1999 ‘Improved fast correlation attack on stream ciphers via convolutional codes’, Advances in Cryptology - EUROCRYPT’99, number 1592 in Lecture Notes in Computer Science , pp. 347–362.

[8] Johansson, T. and Jonsson, F. 1999 ‘Fast correlation attacks based on turbo code techniques’, Advances in Cryptology - CRYPTO’99, number 1666 in Lecture Notes in Computer Science, pp. 181–197.

[9] Courtois, N. and Pieprzyk, J. 2002 ‘Cryptanalysis of block ciphers with overde-fined systems of equations’, In Advances in Cryptology – ASIACRYPT 2002, number 2501 in Lecture Notes in Computer Science, pages 267–287. Springer Verlag.

[10] Courtois, N. and Meier, W. 2003 ‘Algebraic Attacks on Stream Ciphers with Linear Feedback’, Advances in cryptology– EUROCRYPT 2003, Lecture Notes in Computer Science 2656, pp. 345-359, Springer.

[11] Courtois, N. 2003 ‘Fast Algebraic Attacks on Stream Ciphers with Linear Feedback’, advances in cryptology– CRYPTO 2003, Lecture Notes in Computer Science 2729, pp. 177-194, Springer.

[12] Lee, D. H. et al. 2004 ‘Algebraic Attacks on Summation Generators’, In FSE 2004, number 3017 in Lecture Notes in Computer Science, pages 34–48. Springer Verlag.

[13] Meier, W. , Pasalic E. and Carlet, C. 2004 ‘ Algebraic attacks and decomposition of Boolean functions’, In Advances in Cryptology - EUROCRYPT 2004, number 3027 in Lecture Notes in Computer Science, pages 474–491. Springer Verlag.

[14] Armknecht, F. 2004 ‘Improving Fast algebraic Attacks’, In FSE 2004, number 3017 in lecture Notes in computer Science, pages 65-82. Springer Verlag.

[15] Carlet, C. 2001 ‘On the cost weight divisibility and non linearity of resilient and correlation immune functions’, Proceeding of SETA’01 (Sequences and their applications 2001), Discrete Mathematics, Theoretical Computer Science, Springer p 131-144.

[16] Belmeguenaï, A., Derouiche, N. and Redjimi, M. 2011 ‘Image Encryption Using Stream Cipher Algorithm with nonlinear filtering function’, in IEEE High Performance Computing and Simulation (HPCS), 2011 International Conference. 2011, IEEE: Istanbul. Turkey - p. 830 - 835

[17] Berlekamp, E. R. 1968 ‘Algebraic Coding Theory’, Mc Grow- Hill, New- York.

[18] Siegenthaler, T. 1984 ‘Correlation-immunity of nonlinear combining functions for cryptographic applications’, IEEE Trans. Inform. Theory IT-30, 776-780.

[19] Strassen, V. 1969 ‘Gaussian elimination is not optimal’, Numerische Mathematik, 13:354-356.