Journal of Theoretical and Applied Information Technology
15 July 2012. Vol. 41 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN IMAGE ENCRYPTION APPROACH USING STREAM CIPHERS BASED ON NONLINEAR FILTER GENERATOR

BELMEGUENAÏ AÏSSA, DEROUICHE NADIR, REDJIMI MOHAMED

Laboratoire de Recherche en Electronique de Skikda, Université 20 Août 1955- Skikda BP 26 Route d'El-hadaeik, Algérie.

E-mail : belmeguenaiaissa@yahoo.fr , nadirouiche@yahoo.fr , redjimimed@yahoo.fr

ABSTRACT

In this work a novel image encryption scheme using stream cipher algorithm based on nonlinear filter generator is considered. In this work a novel image encryption scheme is proposed based on stream cipher algorithm using pseudorandom generator with filtering function. This algorithm makes it possible to cipher and decipher images by guaranteeing a maximum security. The proposed cryptosystem is based on the use the linear feedback shift register (LFSR) with large secret key filtered by resilient function whose resiliency order, algebraic degree and nonlinearity attain Siegenthaler's and Sarkar, al.'s bounds. This proposed scheme is simple and highly efficient. In order to evaluate performance, the proposed algorithm was measured through a series of tests. Experimental results illustrate that the scheme is highly key sensitive, highly resistance to the noises and shows a good resistance against brute-force, statistical attacks, Berlekamp-Massey Attack, algebraic attack.

Keywords: *Cryptosystem, Decryption, Image correlation, Image encryption, key Stream, Nonlinear Filter Generator, Stream Cipher.*

1. INTRODUCTION

The proliferation of the terminals of access to information as well as the use growing of telecommunications (implementing electronic transfers of information of characters personal) force to have reliable techniques, made safe and commonly accepted. In fact, the use of a communication network exposes the exchanges at the certain risks, which require the existence of adequate security measures. For example, the images to be transmitted can be recorded and copied during their course without losses of quality. The pirated images can be thereafter the subject of an exchange of information and illegal numerical storage. It is thus necessary to develop a tool for protection effective of the data transferred against the intrusions arbitrary. The encryption of the data is very often the only effective means to answer these requirements.

In this work, we are interested in the security of the data images, which are regarded as particular data because of their sizes and their information which is two-dimensional and redundant natures. These characteristics of the data make the classical cryptographic algorithms such as DES, RSA, and ... are inefficient for image encryption due to image inherent features, especially high volume image data. Many researchers proposed different image encryption schemes to overcome image encryption problems [1, 2, 3, 4].

In this research we have tried to find a simple, fast and secure algorithm for image encryption using nonlinear filter generator (NLFG) based on linear feedback shift registers (LFSRs) with a large secret key space filtered by resilient function satisfying all the cryptographic criteria necessary carrying out the best possible compromises. Finally, this algorithm is robust and very sensitive to small changes in key so even with the knowledge of the key approximate values; there is no possibility for the attacker to break the cipher.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. NONLINEAR FILTER GENERATOR

This system was proposed by Siegenthaler [5] to increase the linear complexity of the binary sequence produced by linear feedback shift register (LFSR). A single register (LFSR) is used, length L, producing a binary sequence in maximum period. Certain stages of this register (LFSR) are combined by a nonlinear function f. Such function is called filtering function, must be a high algebraic degree, balancedness, good correlations immunity, high non linearity and preferably to have good algebraic immunity to resist certain attacks [6, 7, 8, 9]. The sequence produced by the function which will constitute the key-stream, combined with the plaintext. We refer to [10, 11] for further details. The linear complexity of the key-stream is at most $\Lambda(s)=\sum_{i=1}^{d}\binom{L}{i}$, where d is the degree algebraic of f.

2.1. Linear Feedback Shift Register (LFSR)

Linear feedback shift register produce a sequence $s=s_0,s_1,...,$ satisfying the linear recurrence relation $s_n=\sum_{i=1}^{L}c_i s_{n-i}$, $n\geq L$, where L is the length of the LFSR, $c_i\in F_2$ for $i=1,...,L$ and $s_i\in F_2$, $i\geq 0$.

The L stages, $S_n=(s_n,...,s_{n+L-1})$, is called a state of the shift register and we note $S_n=(s_n)_{n=0}^{\infty}$ the state sequence. We define the feedback polynomial to be $p(X)=1+c_1X+c_2X^2+...+c_LX^L$. The first output symbols $s_0,s_1,...,s_{L-1}$, are initially loaded into the LFSR, these symbols are called the initial state. This is also the secret key of the LFSR.

The sequences $s=s_0,s_1,...$ produced by LFSR have many interesting properties such as a long periodicity. If the feedback polynomial p is primitive the period is 2^L-1.

2.2. Nonlinear Boolean Function

Nonlinear Boolean function purpose in key stream generators is to hide the linearity introduced by the LFSRs. A Boolean function is function $f:F_2^n\rightarrow F_2$. The function f can be represented uniquely by a multivariate polynomial over F_2 of the form:

$$f(x_1,...,x_n)=a_0+\sum_{i=1}^{n}a_i x_i+\sum_{1\leq i\prec j\leq n}a_{ij}x_i x_j+...+a_{12...n}x_1x_2...x_n.$$

Where the coefficients $a_0, a_i, a_{ij}, ..., a_{12...n}$ belong to F_2. The degree of this polynomial is called the algebraic degree or simply degree of f, and it is denoted by $\deg(f)$. The functions of degrees at most one are called affine functions.

3. METHOD

We used stream ciphers based on nonlinear filter generator for constructing our new approach. The layout of our method is presented in figure 2. In this paper all sequence elements are considered over the field F_2 which consists of the two elements {0, 1}. In this scenario we suppose that the secret key K is used to initialize the stages $s=s_0,s_1,...,s_{L-1}$ of the LFSR of the NLFG at time $i=0$.

Let X a plain-image (i.e. original image) of $n\times m$ pixels. First, sender transforms the plain image X into binary array ((i.e. plain image digit). Let x_i, y_i and z_i be the plain image digit, cipher image digit and key stream digit at time i. Then the encryption process can be described by the equation

$$y_i=x_i\oplus z_i \quad (1)$$

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

$$x_i=y_i\oplus z_i \quad (2)$$

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 X of $n\times m$ pixels.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 [12].

3.1. Key K

Our algorithm is aimed at offering medium term security, which is reflected in the length of 607 bits of secret key $K = k_1, k_2, ..., k_{607}$. 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 brute-force attack.

3.2. LFSR

We considered the linear feedback shift registers of length 607 bits to produce a binary sequence. The feedback polynomial of LFSR is chosen to be the primitive polynomial:

$$p(x) = x^{607} + x^{105} + 1 \quad (3)$$

The initial state of LFSR is never allowed to be the all zero state. It follows that LFSR produces a maximum-length sequence of period $2^{607} - 1$.

3.3. Filtering Function

The filtering function used for generating the key stream is a Boolean function f from F_2^{13} into F_2. At each time i, 13 bits are taken from the LFSR, put into the word $\overline{u_i} \in F_2^{13}$ and input to the Boolean function to calculate the key stream z_i as follows:

$$z_i = f(\overline{u_i}) \quad (4)$$

In this formula, the input word $\overline{u_i}$ is selected as follows from the LFSR stream:

$$\overline{u_i} = \begin{pmatrix} s_i, s_{i+7}, s_{i+13}, s_{i+21}, s_{i+31}, s_{i+41}, s_{i+61}, s_{i+91}, \\ s_{i+111}, s_{i+131}, s_{i+161}, s_{i+221}, s_{i+321} \end{pmatrix} \quad (5)$$

The filtering function f used in our approach is presented in [13]. 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. Encryption and Decryption Image Algorithm.

Encryption

1. *Load the plain image(i.e. Original image);*
2. *Transform the plain image into column digit (i.e. plain image digit) and to store them in* x *;*
3. $N \leftarrow$ *the length of* x *;*
4. *for* $i = 1$ *to* N *to make ;*
5. *To generate the key stream* $z(i)$ *as show the algorithm 3.5 ;*
6. *End to make ;*
7. *for* $i = 1$ *to* N *to make*
8. *Calculate the cipher image digit using relation* $y(i) = XOR(x(i), z(i))$ *;*
9. *End to make ;*
10. *Sent the cipher image digit.*

Decryption

1. *Load the cipher image digit* y
2. $N \leftarrow$ *the length of* y *;*
3. *for* $i = 1$ *to* N *to make ;*
4. *To generate the key stream* $z(i)$ *as show the algorithm 3.5 ;*
5. *End to make ;*
6. *for* $i = 1$ *to* N *to make;*
7. *Calculate the decipher image digit using relation* $x(i) = xor(y(i), z(i))$ *;*
8. *End to make ;*
9. *To put the decipher image digit* x *in the form of image of* $n \times m$ *pixels and to store it in* X *.*

3.5. Key Stream

Inputs:

- x *: plain image digit;*
- $s_0, s_1, ..., s_{L-1}$ *are initially loaded into the LFSR;*
- f *: filtering function with a 13 variables.*

Results:

- s *: binary sequence produced by LFSR ;*
- z *: Key stream produced by* f *.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Treatment:

1. *To read* N *, the length of plain image digit of* x *;*
2. *Introduce the secret key, the value of initialization of LFSR* $s_0, s_1, ..., s_{L-1}$ *;*
3. *for* $i = 1$ *to* $N + L - 1$ *to make;*
4. *Generate the binary sequence* $s(i)$ *produced by LFSR* ;
5. *End to make ;*
6. *for* $i = 1$ *to* N *to make;*
7. *Generate the key stream* $z(i)$ *produced by function* f *;*
8. *End to make.*

4. Experimental Results

Simulation was carried out using MATLAB V 7.5. A number of images are encrypted by the proposed method, and visual test is performed. Three examples are shown in figure 3 (a), 3(d) and 3 (g), where each image is a 256-level gray scale image with the size respectively 256x256 , 128x128 and 95x96 pixels.

4.1. Visual testing

From the original images shown in figure 3 (a), 3(d) and 3 (g), we applied our Encryption algorithm with a secret key 607 bits in order to obtain the cipher images illustrated by the figure 3 (b), 3(e) and 3 (h). By comparing the original images and the encrypted images in figure 3, there is no visual information observed in the encrypted image, we notice that initial information is not any more visible. From the cipher images illustrated by the figure 3 (b), 3(e) and 3 (h), we apply the decrypted algorithm with the same key 607 bits in order to obtain the deciphered images shown in figure 3 (c), 3(f) and 3 (k).

Difference between plain images and their decrypted images shown in fig 3, are illustrated in figure 4, are prove that, there is no loss of information, the difference is always 0.

5. Security Analysis

A good encryption procedure should be robust against all kinds of cryptanalytic, brute-force (exhaustive research) and principal attacks (Berlekamp-Massey Attack, algebraic attack). In this section, the performance of the proposed image cryptosystem 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.

5.1. Key Space Analysis

For secure image encryption, the key space should be large enough to make the exhaustive research attack infeasible. Since the algorithm has a 607 bits key, the intruder needs 2^{607} tests by exhaustive research. An image cipher with such as a long key space is sufficient for reliable practical use.

5.2. Berlekamp-Massey Attack

For a filtering function of degree d , the linear complexity $\Lambda(s)$ of the resulting key stream is upper bounded by $\sum_{i=1}^{d} \binom{L}{i}$. Moreover, it is very likely that the $\Lambda(s)$ of the key stream $(z_i)_{i\geq 0}$ is lower bounded by $\binom{L}{d}$ and that its period remains equal to $2^L - 1$. The Berlekamp-Massey attack [14] requires $2\Lambda(s)$ data and has a complexity of $\Lambda(s)^2$. Using the parameters L = 607; d = 7, linear complexity $\Lambda(s)$ is between 2^{52} and 2^{53}, it is sufficiently large. This complexity completely excludes to use the Berlekamp-Massey attack.

5.3. 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:

$$z_0 = f(K) \ ;$$
$$z_1 = f(h(K)) \ ;$$
$$\dots \ ;$$
$$z_i = f(h^i(K)),$$

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

key of size L bits and equations of d degree is given by $C(L,d)=\left(\sum_{i=0}^{d}\binom{L}{i}^{w}\right)=L^{w.d}$, 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 filtering function. We employ here the expression of Strassen [15] which is $w=\log_2(7)\approx 2.807$.

In our cryptosystem the secret key is 607 bits and the algebraic immunity of the filtering function is equal to 6. This leads to algebraic attack with a complexity which is between 2^{155} and 2^{156}, which is sufficiently large. It is not easy to make a linear approximation of the filtering function within the framework of algebraic attack.

5.4. Histogram Analysis

In the experiments, the plain 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 respective histograms of the plain 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 plain images, 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 images. Some gray-scale values are still not existed in the encrypted images although the existed gray-scale values are uniformly distributed

5.5. Correlation Coefficient Analysis

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

Table 1 gives the corresponding correlation coefficient between plain images and their encrypted images shown in figure 3. It is observed that the correlation coefficient is a small correlation between plain images and encrypted images.

5.6. Image Entropy

It is well known that entropy is measures the uncertainty association with random variable. 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:

$$E(m)=\sum_{i=0}^{G-1}p(m_i)\log_2\frac{1}{p(m_i)} \qquad (6)$$

Where G 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 values of entropy of plain images and values of entropy of their encryptions images shown in fig 3. The values of entropy of encryptions images 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.

5.7. Sensitivity analysis

An ideal image encryption procedure should be sensitive with the secret key. It means that the change of a single bit in the secret key should produce a completely different cipher image. Figure

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6 shows 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.

Table 3 gives the values of entropy of decrypted images with wrong key shown in fig 6 (a), (c) and (e).

5.8 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.e and 3.h, we added a noise of the same size of plain-images. The results are given in the figure 7.a and 7.c. From the images 7.a and 7.c, we apply the decryption algorithm; we have the results illustrated in figure 7.b 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 the case examined, we can note that the deciphered images presented in figures 7.b and 7.d are identical to the original images (see 3.d and 3.g).

6. CONCLUSION

In this Work, a new algorithm based on stream cipher using nonlinear filter generator for image data was introduced; simulations were carried out for 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 attacks. The proposed filtering function verified all criteria cryptographic enough to resist Berlekamp-Massey Attack and algebraic attack. In addition, this method is very simple to implement, the encryption and decryption of image.

Here the security aspects like key space, statistical, Berlekamp-Massey, algebraic, noise analysis and sensitivity with respect to key, are discussed with examples. It is seen that the present cryptosystem is secure against the statistical, brute force, cryptanalytic attacks and to resists the additive noises.

REFRENCES:

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

[2] A. Jolfaei and A. Mirghadri, "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, 2010, pp. 279–285.

[3] A. Jolfaei and A. Mirghadri, "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, 2010.

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

[5] T. Siegenthaler, "Cryptanalysis representation of nonlinearly filtered ML-sequences", In : *Advances in cryptology- EUROCRYPT' 85*, Lectures Notes in Computer science 219,pp 103-110,Springer Verlag, 1986.

[6] T. Siegenthaler, "Decrypting a class of stream ciphers using cipher text only", *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.

[7] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers", *Lecture Notes in Computer Science*, Number 561, Springer Verlag, August 1991.

[8] N. Courtois and W. Meier, "Algebraic Attacks on Stream Ciphers with Linear Feedback", *Advances in cryptology–EUROCRYPT 2003*, Lecture Notes in Computer Science 2656, pp. 346-359, Springer,2002.

[9] N. Courtois, "Fast Algebraic Attacks on Stream Ciphers with Linear Feedback", *advances in cryptology–CRYPTO 2003*,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Lecture Notes in Computer Science 2729, pp. 177-194, Springer, 2003.

[10] P.van Orschot A. Menezes and S. Vantome, "Handbook of applied cryptography", Available: htt.www.cacr.math.uwaterloo.ca/,1996.

[11] G. Ars, "une application des bases de Gröbner en cryptographie", *DEA de Renne I*, 2001.

[12] C. Carlet, "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, 2001.

[13] A. Belmeguenaï, N. Derouiche and M. Redjimi, "Image Encryption Using Stream Cipher Algorithm with nonlinear filtering function", *Proceedings of The 2011 International Conference on High Performance Computing & Simulation*, HPCS 2011), July 4 – 8, 2011, P 830-835 ,Istanbul, Turkey.

[14] E.R Berlekamp. "Algebraic Coding Theory", *Mc Grow- Hill, New- York*, 1968.

[15] V. Strassen, "Gaussian elimination is not optimal", *Numerische Mathematik*, 13:354-356, 1969.

Journal of Theoretical and Applied Information Technology
15 July 2012. Vol. 41 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

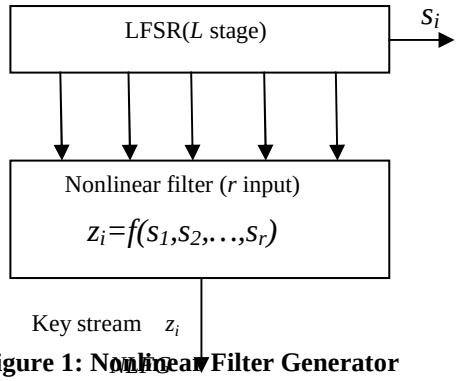

Figure 1: Nonlinear Filter Generator

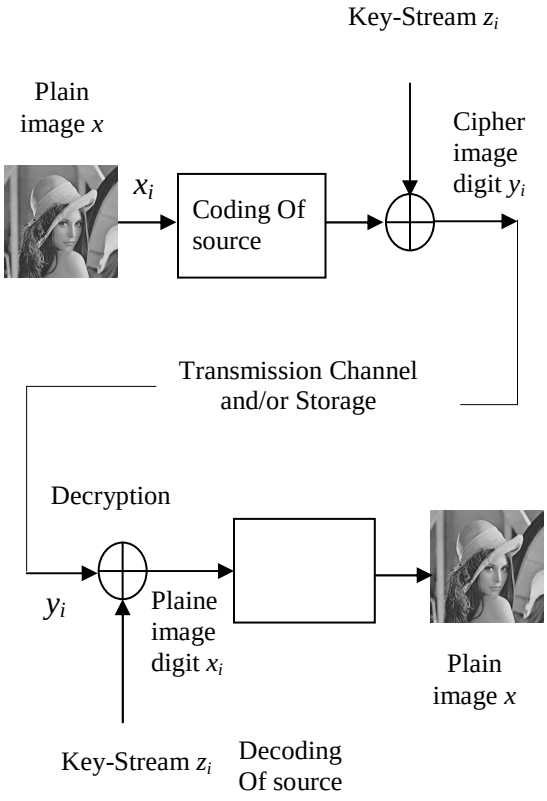

Figure 2: Block Diagram of the Proposed Cryptosystem

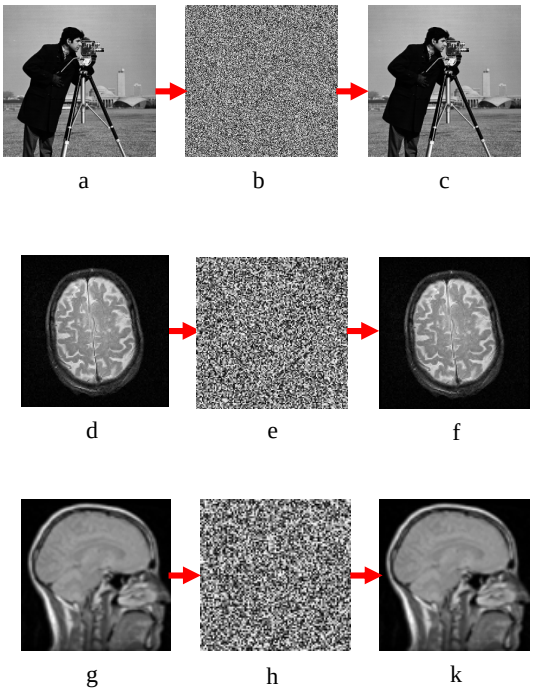

Figure 3.Visual testing: Frame (a), (d) and (g) Gray image show the original image, frame (b), (e) and (h) respectively show the encrypted image, frame (c), (f) and (k) respectively show the decrypted image.

Journal of Theoretical and Applied Information Technology
15 July 2012. Vol. 41 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

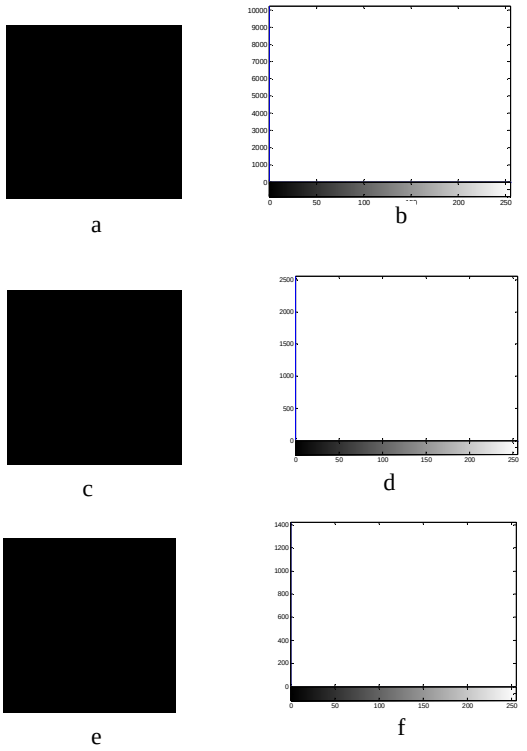

Figure 4. : Frame (a), (c) and (e) respectively show the difference between original image shown in fig 3(a), (d) and (g), and their decrypted image shown in fig 3(c), (f) and (k). Frame (b), (d) and (f) respectively show histogram difference of (a), (c) and (e).

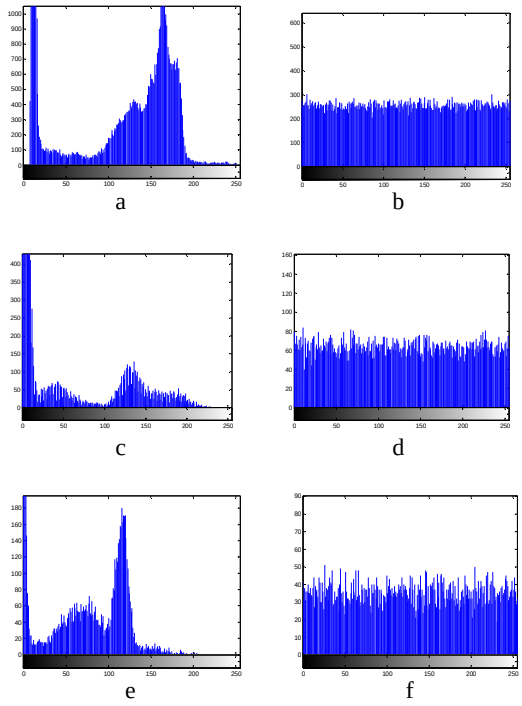

Figure5. Histogram analysis: Frame (a), (c) and (e) respectively, show the histogram of the plain images shown in fig 3(a), 3(d) and 3(g). Frame (b), (d) and (f) respectively; show the histogram of the encrypted images shown in fig 3(b), 3(e) and 3(h).

Table 1. Correlation Coefficients analysis

Cases	Correlation coefficient
Image 3.a	-0.0014
Image 3.d	0.0045
Image 3.g	-0,0011

Table 2. Image Entropy

Plain-Image	Entropy	Encrypted Image	Entropy
Image 3.a	7.0097	Image 3.b	7.9973
Image 3.d	6.3454	Image 3.e	7.9904
Image 3.g	6.6150	Image 3.h	7.9796

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

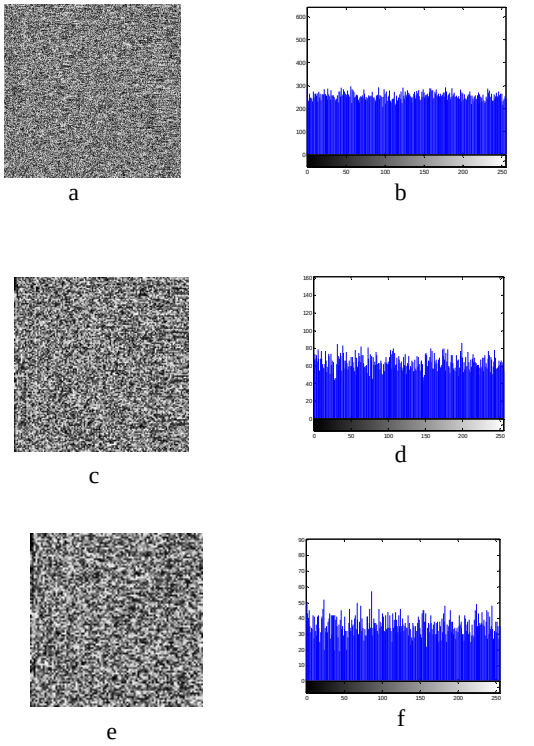

Figure 6. Sensitivity analysis: Frame (a), (c) and (e) respectively, show decrypted image with wrong key of the encryption images shown in fig 3(b), 3(e) and 3(h). Frame (b), (d) and (f) respectively, show histogram of images (a), (c) and (e).

Table 3. Image Entropy

Cases	Entropy
Image 6.a	7.9970
Image 6.c	7.9881
Image 6.e	7.9786

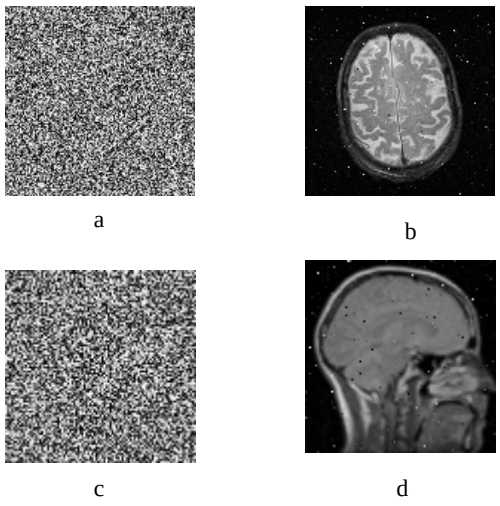

Figure 7. Noise Analysis: Frame (a) and (c) respectively, show cipher image shown in fig 3(e) and3(h) with noise added. Frame (b) and (d) respectively, show their decrypted images