Comparison of Serpent, Twofish and Rijndael encryption algorithms in tele-ophthalmology system

Mohammadreza Naeemabadi, Behnam Sadeghi Ordoubadi, Alireza Mehri Dehnavi and Kambiz Bahaadinbeigy

Young Researchers and Elite Club, Majlesi Branch, Islamic Azad University, Isfahan, Iran.
Medical Image & Signal Processing Research Center, Isfahan University of Medical Sciences, Isfahan, Iran.
Department of Biomedical Engineering, School of Advanced Medical Technologies, Isfahan University of Medical Sciences, Isfahan, Iran.
Medical Informatics Research Center, Kerman University of Medical Sciences, Kerman, Iran.

ABSTRACT

Introduction: Considering the development of telemedicine systems in Ophthalmology, preserving the privacy, Security of personal data and patients’ electronic records from secondary changes is undeniably essential. Cryptographic systems are one of the most available and safest procedures to satisfy these needs.

Methods: In this study, the three powerful encryption algorithms, Rijndael, Twofish and Serpent are used for encrypting the images of retina. Indeed, we used seven criteria of encryption quality, cross-correlation, entropy analysis, Key Sensitivity, Noise Sensitivity, plaintext sensitivity and Throughput, to evaluate these methods.

Findings: In assessments, we observed Rijndael encryption algorithm represents higher encryption speed and considerable simplicity; In addition, considering output entropy, it is superior to the other two algorithms. Although, in comparison to Rijndael, Serpent encryption algorithm has shown a considerable lower speed in compare with Rijndael. Serpent has reduced the correlation between plaintext and encrypted images more than other mentioned algorithms. Two fish encryption algorithm, compared to the two other algorithms, showed a significantly lower noise sensitivity. Conclusion: However, in terms of throughput and quality of encryption, Two fish encryption algorithm has appeared weaker in results; this must be considered that all these three algorithms have provided all the conditional security so that, no practical attacks have been able to break them so far. Therefore, the higher noise resistance of Two fish encryption algorithm makes it more proper to encrypt the images of retina.

INTRODUCTION

Diabetic retinopathy is one of the most important microvascular effects in 30% to 50% of diabetic patients which is the main factor of blindness in individuals between the ages of 20 to 74 years old (Semeraro, F., et al., 2011). At about 40% of diabetic patients have some degrees of diabetic retinopathy that 8% of them reach the acute levels and even incur blindness (Kempen, J., et al., 2004).

So far, no certain cause is known which leads to diabetic retinopathy. The most important mechanisms can be assume as pathogenesis in the diabetic retinopathy are: Polyol Metabolic Pathway, increases in platelet adhesion, agglutination of red blood cells, changes in blood vessel walls, growth factor and retinal hypoxia in diabetic retinopathy (Duh, E., 2008; Poretsky, L., 2002).

The risk of progression of diabetic retinopathy and blindness can be reduced considerably by periodic examination and early treatment to control severity of disorder. In conducted studies we observed that the risk of vision loss was reduced up to 52% by early diagnosis, control and treatment. The reduction in the rate of blindness, due to diabetic retinopathy, significantly reduced treatment costs (Hazin, R., et al., 2011).

The prevalence and severity of diabetic retinopathy having the disease symptoms even in early stages leads the need for comprehensive retinal examination to make an early diagnosis of diabetic retinopathy (Semeraro, F., et al., 2011). For this purpose, different associations such as American Diabetes Association, American
Academy of Ophthalmology, Accreditation & Health Evaluation Health Product (ANAES), French Agency for the Safety of Health Product (AFFSAPS), National Eye Institute, American optometric association and other communities which are professional in this field recommended annual ophthalmologic examination in their guidelines. The major and suggested clinical tests ETDRS, DCCT, DRVS, DRS and UKPDS also revealed in their achievements of the recent three decades that the early control and treatment of the diabetic retinopathy leads to the reduction of the risk of blindness and vision complexities (Swanson, M., 2005).

However, limitations such as increase in the population of diabetic patients (Due to the increased prevalence of diabetes), reduction of the number of ophthalmologists and visit impossibilities due to deprivation and poverty prevent the spread of annual tests (Chabouis, A., et al., 2009). Utilization of telemedicine solution in ophthalmology increases the promotion of quality and the level of presented services; ensures the access and extent, reduction of costs and the optimal management of resources and requirements (Papageorges, M., P. Hebert, 2001; Li, H.K., 1999; Papageorges, M., P. Hebert, 2001).

Telemedicine Association of USA offers the main equipment of the system for tele-diabetic retinopathy examination as follow:

1) Image Acquisition section (Including cameras, computers and other accessories)
2) Transmission, Storage, retrieve multimedia data section
3) Image analysis and Clinical Workflow Management section (ATA, 2011)

One of the most essential part of this system is the information security section which is responsible for data protection and privacy. The patient’s medical records contain highly private and sensitive information which must not be the access of the unauthorized people. This inaccessibility of the patient’s medical records not only ensure privacy patient’s records but also protects them against any threat and invasion (Kovacevic, S., et al., 2007; Bouslimi, D., et al., 2012).

It should be mentioned, in most of the studies undertaken in the field of tele-diabetic retinopathy, using a reliable connection channel is regarded obligatory. Steven D Schwartz, in his study discussed transferring taken images via internet through secure communication channel, without a detailed description of the mode and procedure of the reliable connection platform (Schwartz, S.D., et al., 2000). Alexandra Lajoie has also discussed sending images via a security system without a detailed description (Lajoie, A., et al., 2008).

Massin used OPHCARE software to send images which secures transmitted data by 128-bits encryption algorithm (Massin, P., et al., 2004). OPHDIAT tele diabetic retinopathy system, also employed 128-bits encrypting system to guarantee security of sent information (Massin, P., et al., 2008).

In this study, we compared three common and robust algorithms of the world and surveyed them according to the medical priorities.

In the second section, the three encryption algorithms are defined and later discuss the above mentioned algorithms’ implementation. The data used in this study are introduced in the third section. In the fourth section, firstly the evaluation criteria are introduced and then at the end of the section, the results of these criteria are investigated. At last these algorithms are challenged according to the requirements of a system for tele-ophthalmology.

Method:

As mentioned before in this section three encryption algorithms, are comprehensively introduced and explained about implementation of each one.

2-1. Rijndael Encryption:

Rijndael Encryption Algorithm developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, to participate in the Advanced Encryption Standard contest that after three steps and the Completion, this algorithm was selected. At that time, when most of encryption algorithms introduced based on Feistel Network, Rijndael Encryption Algorithm designers, broke the tradition and by presenting the algorithm structure based on the substitution – permutation network, went on a great risk. According to conditions are determined by NIST, this algorithm benefits from 128-bits block size and 128, 192 and 256 bits as key size; While the number of rounds changes according to the key length and is defined for the mentioned lengths as 10, 12 and 14, respectively. This algorithm is based on modular basis function and Galois finite field GF (2^8) and the basis of calculations in Rijndael is defined based on byte calculations (8 bits).

Rijndael encryption algorithm consists of three distinct parts, primary round, main round and final round. In the primary round, only the round key XOR with the input block and somehow the input whitening action is performed in this turn, therefore this round is not considered in counting the number of rounds. Figure 1 shows these three parts by a block diagram.

Main round consist of four sequential steps, respectively, byte substitution (Sub Bytes), row shift (Shift Rows), linear transformation of columns (Mix Columns) and XOR with the round key (Add Round Key). The final round is very similar to the main round with the difference that the third stage, combined with the round
key, is omitted in this round (Daemen, J., V. Rijmen, 2002; Daemen, J., V. Rijmen, 1998; Daemen, J., V. Rijmen, 2011).

Fig. 1: Rijndael Encryption Algorithm

2-2. Serpent Encryption algorithm:

Serpent Encryption algorithm was first introduced by Ross Anderson, Eli Biham and Lars Knudsen to participate in the competition, advanced AES encryption algorithm. This team are also designer of other encryption algorithm such as LION, Tiger, Pik, Py, SHAVite-3, DEAL and Grostl.

According to the terms and conditions defined by NIST, this algorithm supports Input 128-bits block and key length of 128, 192 and 256 bits. The unique, 32-bit, design of this algorithm let it complete the 32 round algorithm, designed based on semi substitution – permutation network in the minimum time. Figure 2 shows the block diagram of the Serpent algorithm.

In serpent Encryption algorithm, two blocks, preprocessing and post-processing, perform the 32 operational rounds before and after the beginning, respectively. These blocks are called Initial permutation and final permutation. These two permutations which are located at the algorithm, like the permutations are used in DES have no value of security and encryption and are designed to improve the computational efficiency that could be removed in the Bit Slice processes. Regarding to the fact that, Serpent does not use the Feistel network, all data lines’ width are equal to the size of input block, that is 128-bits data block.

Fig. 2: Serpent Encryption Algorithm

Rounds in Serpent, consists of three steps, key mixing, substitution and linear transformation and in the last round is a little different from the previous ones, in this round after substitution of key mixing used instead of linear transformation. Each of the 31 primary rounds use one of round key and the final round uses two round key, so, thirty three 128-bits round keys must be generated in the key expansion stage (Anderson, R., et al., 1998).

We could indicate the rounds in Serpent by mathematic relations based on 1. In 1 offers two different definitions for the round transform. The first one is for the primary 31 rounds and the second one presents the final round which has become the second mixing with the key instead of the linear transformation. At the 1 relation, L is linear transformation, Ki is i-th round and Si is the substitution for i-th round (Elbirt, A.J., C. Paar, 2000; Biham, E., et al., 1998).
\[ R_i(X) = L(S_i(X \oplus K_i)), \quad i = 0, \ldots, 30 \]
\[ R_3(X) = S_i(X \oplus K_i) \oplus K_{32}, \quad i = 3 \]

(1)

The linear transformation used in this algorithm could be seen in the figure 3.

**Fig. 3:** Linear Transformation in Serpent

2-3. Two fish Encryption Algorithm:

Two fish is a symmetric key block cipher that like any of AES selected encryptions uses a block size of 128 bits and key sizes of 128, 192 and 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest. This algorithm, in structure, is based on Blowfish and Bruce Schneier has introduced it as the Blowfish’s evolutionary Algorithm. The repetition of Feistel network for 16 times (16 rounds) has attempted to provide its best strength and capability. The structure of the Feistel network in this algorithm is presented in the figure 4.

**Fig. 4:** Two fish Encryption Algorithm
First the input 128-bits block is divided into 4 blocks of 32-bits. At first it seems that the designers has attempted to change the network of Feistel structure in Two fish but with a more attention we realize that the structure used is exactly the same and half a block is added to the Feistel structure. These two half blocks themselves are divided into two portions which here are called lower block ($R_{r,1}$) and upper block ($R_{r,0}$). In Twofish, like Serpent, a pair of pre-processing and post-processing blocks is used, which in whitening is done by XO Ring operation with 128-bits key in the data block.

In Two fish, the Feistel function itself consists of 4 sequential operations, Primary rotation, $g$ function, Pseudo Hadamard Transforms, The combination of the key and the final rotation (Schneier, B., et al., 1999; Schneier, B., et al., 1998).

2-4. Implementation of Rijndeal, Two fish and Rijndael Encryption:
In this study, the algorithms are implemented in MATLAB software, because the data are color images of retina and, compared to other softwares such as Visual Studio, analyzing them by this software is more conceivable due to its powerful libraries. Moreover, we have done all the calculations as 32 for the algorithms be of higher speed. Moreover, all of the written scripts are compatible with multi-core processors.

Unfortunately, none of these algorithms, Serpent, Two fish, and Rijndael has not been implemented in MATLAB yet and it was required to basically write all of these algorithms on MATLAB.

In the process of implementing these three algorithms, first, each of the algorithms is implemented as block to block, based on the pseudo-code that its designers had provided.

The performance accuracy of each block is compared to its output according to the pre-collected input-output table. These tables are mostly prepared to each block by the designers or are obtained by the handy calculations based on the mathematical relations of the algorithm.

3- Data:

In this study, 4 retina image database, which taken by Fundus cameras, are used to assess encryption algorithms. DIARETDB1 (Kauppi, T., et al., 2007), DRIVE (Staal, J., et al., 2007), Eye Scan (Ting, D.S., et al., 2012), STARE (Hoover, A., et al., 2000) are databases which totally consist of 164 retina images are used in the study. Preceding analyzing and evaluating, all the images transform to the standard Non-compressed TIF format and the analysis is performed in this format and in RGB color environment.

The DRIVE data consists of 40 images of retina including extracted vessels. These data are rather used to study the extraction of the vessels in the retina by fundus cameras.

![Fig. 5: Part of DRIVE dataset, retina image including vessels marked image](image)

All the images are taken by the CANON CR5 non-mydratic camera which is equipped with a 3CCD sensor. The taken images are single field and of 45$^\circ$. The images are presented in 565 × 584 pixels dimension having a color depth of 24bits. Moreover, along with each of these images, there is an image which shows the vessels that are taken away manually.

DIARETDB1 dataset consists of 89 Fundus color image, which 84 images of them represent mild Proliferative diabetic retinopathy and the remained 5 images are without any degrees of diabetic retinopathy. DIARETDB1 is typically used to studies on diabetic retinopathy.

The images are taken by a Fundus camera at the 50 $^\circ$ field at the Hospital of Kuopio University in Finland. The images are provided in the size of 1500 × 1152 pixels with the color depth of 24-bits in the standard compression format of PNG.

It should be mentioned, each image is attached with a paired marked image, refers to the existing place of the hard exudates hemorrhage and micro aneurysm in fundus images. The marked images are provided by a software toolkit which was along with the set.

The STARE data set consists of 20 fundus images of retina which are acquired by Fundus Topcon TRV-50 camera.
Any of the images in STARE are provided in 605 × 700 pixels and a color depth of 24 bits. This point should be considered that the taken images are saved and provided in ppm format. A set of manually marked images is presented that shows the vessels in the corresponding image.

The EYESCAN data set consists of 15 images in the dimensions of 2392 × 1944 pixels and the color depth of 24-bit which are part of the data set developed by the research team at the University of Melbourne in their Diabetic Retinopathy Studies by Merge Eye Scan device.

4- Assessment and Outcomes:

So far, several methods are presented for statistical assessment of cryptographic algorithms. In this study, Encryption Quality, Cross Correlation, Entropy Analysis, Plaintext Sensitivity, Key Sensitivity, Noise Sensitivity and Throughput are assessed.

4-1. Encryption Quality:

In fact, encryption quality shows the mean difference between the histogram of the plaintexts and ciphertext. In this study the quality of encryption is computed based on relation (2).

\[ EQ = \frac{\sum_{i=0}^{255} |Hist(P)_i - Hist(C)_i|}{256} \] (2)

In relation (2), Hist (P) and Hist(C), respectively, are the histograms of the plaintext and ciphertext. The parameter measures the changes in the histogram of the encrypted image in comparison to the original one and the higher this value is; the more powerful is the encryption (Ziedan, I.E., et al., 2003; Elkamchouchi, H., M. Makar, 2005).

The results of implementing the encryption in the data quality analysis are shown in the plot drawn in figure 6. Although, the chart indicates the nearly equal encryption quality in all three algorithms, Twofish encryption algorithm reached a quality around 3 percent higher than Rijndael algorithm.

![Encryption Quality](image)

**Fig. 6: Encryption Quality**

4-2. Cross-Correlation Coefficient Factor:

In fact, Cross-Correlation Coefficient Factor is the cross-correlation between plaintext and ciphertext. If cross correlation coefficient factor is closer to one, two images have more similarities; while if this value tend to zero, it represent images are independent to each other and uncorrelated (KG., N., D.V. Ramaswamy, 2009). The cross-correlation between two signals is calculated by relation (3).

\[ R_{xy} = \frac{\text{cov}(x, y)}{D(x) \times D(y)} \]

\[ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \]

\[ D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \]

\[ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \] (3)
Figure 7, shows the correlation between the encrypted image and the original one for each of the three encryption algorithms. Although the images of the before and after the encryption in Rijndael have higher correlation than the two other encryption algorithms, but the difference is inconsiderable, especially between Rijndael and Two fish. As matter of the fact that, Serpent has minimized the value. Considering the fact that Rijndael has presented a cross-correlation of about 0.01, the two images could be almost considered uncorrelated.

![Cross Correlation](image)

**Fig. 7: Results in Cross Correlation**

4-3. **Entropy Analysis:**

Shannon introduced entropy as a measure for the information existing in the source. Entropy is an estimated randomness in images (Mirghadri, A., A. Jolfaei, 2011). Shannon’s entropy is defined as the $H(s)$ of the $S$ massage source in the relation (4).

$$H(s) = \sum_{i=1}^{2^w} P(S_i) \log_2 \left( \frac{1}{P(S_i)} \right)$$

(4)

In the equation 4, $P(S_i)$ is probability of $S_i$ and entropy is expressed in bits. The criterion of output entropy, in fact, refers to the entropy of the encrypted image passing through nonlinear transformation, (in this study, the three encryption algorithms), that the results are shown in figure 8.

![Entropy Results](image)

**Fig. 8: Entropy Results for Encryption Algorithms**

The figure indicates the Rijndael entropy is considerably higher than Two fish. This means that Rijndael encryption algorithm has succeed to distribute the information in the image (leveling out the texture of the image) at about 127% more than Two fish and about 40% more than Serpent.

4-4. **Throughput or Output rate:**

Throughput or output rate is one of the most important parameters of an encryption which depends on the number and the type of the operations that takes place in an encryption.

In any encryption system, it is desirable that the plaintext be encrypted fast and with the high quality of encryption. All cryptographic algorithms try using a set of non-linear functions that are repeatedly applied, to
create clutter and rupture in the encrypted text. Considering the number of operations required per cycle, at each round of the algorithm, the process need a certain computational complexity and a certain time to operate. By increasing the number of rounds, the spent time increases as a multiple of the number of rounds. Therefore, algorithm designers try to reduce the spent time by creating an interaction between the complexity and the number of the rounds along with offering desirable encryption quality. The time spent for each block of input data is inversely related to the output rate (Ahmed, HE-dH., H.M. Kalash, Allah OSF, 2006).

In figure 9, is observed the throughput of Rijndael considerably higher than Serpent and Two fish. In fact, Rijndael is 20 times faster than Two fish and 10 times faster than Serpent which this rate is remarkable.

\begin{center}
\includegraphics[width=0.5\textwidth]{throughput.png}
\end{center}

\textbf{Fig. 9:} the throughput of cryptographic algorithms in terms of kilobits per second

\section*{4-5. Plaintext Sensitivity:}

Being sensitive to the partial changes in the input data (plaintext) of a cryptographic system, is one of the advantages of an encryption algorithm. Sensitivity degree to changes in input is assessed by computing, mean absolute error (MAE), Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI) per unit change in a given data set. These parameters are introduced by relations (5).

\begin{align*}
\text{MAE} &= \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \left| P(i,j) - C(i,j) \right| \\
\text{NPCR} &= \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} D(i,j) \times 100 \% \\
D(i,j) &= \begin{cases} 0 & \text{if } C(i,j) = C(i,j) \\ 1 & \text{if } C(i,j) \neq C(i,j) \end{cases} \\
\text{UACI} &= \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \left| C(i,j) - C(i,j) \right| \times 100 \% \\
\end{align*}

(5)

In this study, the changes are considered as one bit but the input sensitivity can investigated with more than one bit; hence this feature is added to the analyzer of sensitivity to plaintext (Bouslimi, D., et al., 2012; Ahmed, HE-dH., H.M. Kalash, Allah OSF., 2007). In figure 9, the plot shows the sensitivity to the plaintext among these three based on the mentioned criteria.
Fig. 10: Plaintext sensitivity in terms of MAE, NPCR and UACI

Apparently, Rijndael and Serpent have an equal sensitivity to the plaintext; whereas, compared to changes in the plaintext, Two fish severely indicates less sensitivity in results.

4-6. Key Sensitivity:
The key sensitivity test is very similar to the plaintext sensitivity test so that the changes in the test are in the key. In this test, at first the plaintext is encrypted by key A to obtain the encrypted text and then the plaintext is encrypted again by the key B and the second encrypted text is obtained. A comparison based on, mean absolute error (MAE), mean square of errors (MSE), bits error ratio (BER) and symbols error ratio(SER) is prepared and presented in relations 6 (KG., N., D.V. Ramaswamy, 2009).

\[
MAE = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} |P(i, j) - C(i, j)|
\]

\[
BER = \frac{\text{ErrorBitNumber}}{N} \times 100
\]

\[
MSE = \frac{1}{N} \sum_{i=1}^{N} [P(i) - P'(i)]^2
\]

\[
PSNR = 10 \log \left( \frac{\max(P)}{MSE} \right)
\]  

(6)

The results of the assessment shown in figures 11 and 12 indicate the intense competition between Rijndael and Serpent. In the other hand, Two fish, similar to the Plaintext Sensitivity Test, showed a lower capability. However, despite the diagram shows the lower rate of BER in Two fish, the algorithm has succeeded to distort all the 32-bits symbols.

Fig. 11: Key sensitivity in terms of MAE and MSE
Fig. 12: Key sensitivity in terms of BER and SER

4-7. Noise Sensitivity:

In this study, binary symmetric channel (BSC) model is simulated to evaluate noise sensitivity of each introduced encryption algorithm, through this channel. Thus, the ciphertext passes through this channel with degrees of distortion. Following the decryption, the distorted ciphertext is investigated in the process of encryption to find the differentiations between the generated plaintext and original plaintext. In this test, some changes are assumed to be performed on encrypted data during the process of data transmission through the noisy data channel, then, after decrypting the encrypted data on the other side of the channel, the resulting errors are assessed by the criteria mentioned in Key Sensitivity Test. For binary symmetric channel, noise sensitivity is studied by three different possibilities, 0.1, 0.01, and 0.001.

The results are shown in the diagrams drawn in figures, 13, 14 and 15, which are calculated by the criteria given in relation 6.

Fig. 13: Noise sensitivity in terms of MSE and MAE
In comparison to the other two encryption algorithm, is observed Two fish having less noise sensitivity in the BSC. Therefore, resistance to noise especially in the lower levels of noise in Two fish is obviously high. Although, Two fish has the same ratio of 32-bits symbols distortion as two others in BSC channel, the results presented on the scale of bit and byte are more promising.

Discussion and Conclusion:
In this study, the three powerful encryption algorithms, Rijndael, Two fish and Serpent are used for encrypting the images of retina.

In the results, were observed to have equal characteristics and capacities in general aspect. The results could be summarized in table 1, according to the mentioned tests and the results in section 4. It means, each of algorithms is rated between -1 to 1 in each test to reach an overall assessment. If, the algorithm is superior to the other it assigns 1 score, if, the results are the same assigns 0 and if, it’s weaker than the others assigns -1.

<table>
<thead>
<tr>
<th>Rijndael</th>
<th>Serpent</th>
<th>Twofish</th>
<th>Criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>Encryption Quality</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>Cross</td>
</tr>
</tbody>
</table>

Fig. 14: Noise sensitivity in terms of SER and BER

Fig. 15: Noise sensitivity in terms of PSNR
In the table above, one can see that the Rijndael is the winner of this competition based on statistical criteria. However, the succession is not absolute, because each of the algorithms has different advantages and the criteria are assumed to be equal and without any preferences form each other. Rijndael algorithm owes its superiority over Serpent to its high speed of encryption. Although, the difference may be magnified due to the MATLAB software processing weakness or incompatibility (e.g. the weakness in the ACML library); the balance would not reverse under any circumstances. The main cause of low encryption speed in Serpent are its 4-bits mathematical operations in S-Boxes, which has led each of these to be replaced by at least fifteen 32-bits operations.

Serpent in compared to the other two algorithms, presents higher sensitivity to key and plaintext. Thus is more successful in hiding the pattern.

However, Two fish has shown its weakness for the sensitivity to the plaintext (plaintext and cipher key); it has also shown a lower noise sensitivity and higher encryption quality.

In general, what is observed in these algorithms is that, after a century of study to break them and the development of computer systems and processing systems, no attack has succeed to challenge any of them. At least, these algorithms secure their safety and it severely can be guaranteed for next 20 years. This feature is considered as a boarders of security, so that in case any algorithm follows a set of conditions would own the power and security.

What is missed in these block encryption algorithms’ designation is noise sensitivity. Noise sensitivity is linked to key sensitivity and plaintext sensitivity and both follow the same reason. Two fish algorithm provides less noise sensitivity due to the lower key sensitivity and plaintext sensitivity.

For medical images, it is desired and of high importance to have an image free from noise. While, block encryption algorithms manifold the noise production. Thus, Two fish algorithm could be more appropriate to retina images due to the lower noise sensitivity it presents. However, we have to note that, from a statistical standpoint, though Two fish has shown weaker results; the algorithm is conditionally secured and so far no decryption attacks have succeeded to break it.

**REFERENCES**


