Secure Image Encryption Using Filter Bank and Addition Modulo 2^8 with Exclusive OR Combination

Saleh Saraireh saleh_53@yahoo.com
Department of Communications and Electronic Engineering
Philadelphia University
Amman,Jordan.

Mohammad Saraireh srayreh_2000@yahoo.com
Department of Computer Engineering, Mu'tah University
Karak, Jordan

Yazeed Alsbou yazeed_alsbou@yahoo.com
Department of Computer Engineering, Mu'tah University
Karak, Jordan

Abstract

In this article, the security performance and quality for image encryption and decryption based on filter bank and the combination between XOR and addition modulo 2^8 have been studied and assessed. The most common security parameters for image encryption and decryption have been employed. The parameters have been used to examine the proposed image encryption scheme with one and two rounds. The parameters include histogram, correlation coefficient, global entropy, block entropy, avalanche effect, number of pixel change rate (NPCR), unified average change intensity (UACI), exhaustive key analysis, and key sensitivity test. The simulation results proved that, the image encryption process passes all these tests. Moreover, it reaches or excels the current state of the arts. So the encrypted image becomes random-like from the statistical point of views after encryption.

Keywords: Image Encryption, Filter Bank, XOR, Histogram, Key Sensitivity.

1. INTRODUCTION

The current progress in computer industry and communications permitted digital multimedia applications like image, file transfer, audio, and video to be distributed over different networking technologies. However, the propagation of these applications over these unreliable and public networks has created a suitable medium for unsafe and uncontrollable distribution [1]. Due to this, protection of these information and data from unauthorized users is becoming more important these days. This can be achieved by using Cryptography. Cryptography is a security technique that requires ciphering or encrypting of data. Encryption is employed to preserve information safe during storage and transmission over communication networks. This process has long been employed by militaries, security organizations and governments to support secret communications and information exchange.

Encryption is the process of converting original multimedia information (i.e., plaintext) into another version usually called a ciphertext to make it hard to be understood excluding those who have knowledge called a key. The resulted ciphertext cannot be accessed and read without decrypting it. Decryption is the process of reconstructing the encrypted information (ciphertext) into its original form. Several security approaches have been proposed to insure the required security and protection of information [2]. Generally, encryption techniques span from simple spatial domain approaches to more complicate frequency domain ones [3]. As a result, exploiting of these security approaches permit users to transmit their information and private data over unsecure communication networks without any fear due to attacks or eavesdropper.

Generally, there are two main kinds of data security systems (i.e., cryptography systems: secret key cryptography and public key cryptography. Secret key cryptography (which is also called symmetric key cryptography) is an approach where both the sender and the receiver know the same the key. Data is encrypted in the sender side by a specific key and the encrypted data is decrypted at the receiver using the same key [4]. However, public key cryptography (which also called asymmetric key cryptography) is an approach where keys work by matching public and private keys [4].

Based on that, multimedia encryption methods must ensure end-to-end security when sharing these applications among users over a variety of communication systems [5]. Image is one of the most important multimedia applications that must be protected and secured against unauthorized access and attacks. That is due to images possess significant applications in numerous fields like medical imaging, videoconferencing, tele-medicine, documentation, and military [6]. Due to this, it is crucial to secure and protect the confidential image information.

Multimedia (i.e., Image) encryption schemes must be carefully designed to protect image content [7]. Most of the existing ciphering algorithms are designed for text encryption. These classical encryption methods are not usually appropriate for image ciphering due to image huge amount of data which requires heavy computations [8]. Therefore, various encryption schemes have been proposed recently for the sake of image encryption only.

In [9] an image encryption method based on block transformation algorithm was proposed. In this paper, the original image is splitted into a random number of blocks. These blocks are then shuffled with the image. This image is encrypted by Blowfish algorithm. The importance of this approach is the use of the seed to generate the random number of block sizes used in image transformation process to produce the shuffled image before encryption. The smaller the block size the better the encrypted image.

An algorithm using permutation was to divide the original image into blocks of 4x4 pixels each to produce lower correlation and higher entropy values [10]. These blocks were distributed over the image and the resulted image was then encrypted using the RijnDael algorithm. The strength of this algorithm was the use of the permutation method to generate a new image very different from the original one before encryption. Using the inverse permutation of the blocks, the original image can be decrypted.

In [11] an image encryption scheme based on improved version of the Advanced Encryption Standard (AES) to increase security level for image encryption. The new proposed approach was based on adjusting the Shift Row Transformation. By this, the modified version of the AES produced results compared to the original AES in terms of reducing the statistical attack opportunities by increasing the security level. In [12] filter bank systems were used as a cryptosystem, in this system, the analysis filter banks were employed to make the encryption process, while the synthesis filter banks were employed to achieve the decryption process.

A Modification on Advanced Encryption Standard (MAES) to improve the level of security and to get enhanced image encryption was proposed in [13]. The experimental results illustrated that higher security levels were obtained compared to the AES encryption algorithm.

The authors in [14] devised an image encryption algorithms using public key encryption called Gödelization. The original image was transformed into a sequence called Godel Number Sequence (GNS). Then the transformed image was compressed using Alphabetic coding (AC). Results of this algorithm showed that it performed efficiently for images encryption but with high processing time for large images.

An image encryption technique using two chaotic systems was introduced in [15]. One is used to generate a chaotic sequence to be transformed into a binary stream by a threshold function. The second chaotic system was employed to build a permutation matrix. The image encryption included randomly modification of the original image pixel values using the binary stream as a key stream. Then, the resulted (transformed) image was encrypted again by the permutation matrix.

Moreover, another image ciphering technique was developed in [16]. This scheme was based on extension of chaotic sequences where chaotic cryptography was used and called a key cryptography. The extended chaotic processes were generated by the n-rank rational Bezier curve which provided high key space and good security level for the encrypted image.

In [17] an encryption scheme was devised using logistic map and cheat image. In this method, a confusion and diffusion approach for image encryption was employed. Logistic map is a discrete chaotic system which was used as secrete key. In addition, a cheat images is selected with size as same as the original image. Then the cheat image and the original image were mixed by a permutation. This cheat image, diffusion and confusion matrices were used to cipher the original image. The standard statistical showed that this image encryption algorithm was robust and secure.

New encryption technique by decomposing the original image into 8x8 blocks was proposed in [18]. These blocks were transformed into frequency domain using the Discrete Cosine Transform (DCT). Then, the higher frequencies DCT coefficients were encrypted by Non-Linear Shift Back Register (stream cipher). The resulted encrypted coefficients are shuffled based on a pseudorandom bit sequence. In addition, the developed algorithm was lossless and selective approach which produced a fast encryption process.

The authors in [19] introduced a new image encryption system using the DNA sequences concepts. This approach was used for improving big image encryption time. DNA sequences were used as main keys. Using the one of the DNA sequence, the plain image pixels were scrambled. Then, another sequence was used to produce DNA template to achieve pixel replacement. Then, the new image was XOR bit by bit with one of the encryption templates generated by DNA sequence. This technique had high security against attacks. Additionally, this technique reduced the encryption time with great extent.

In [20] a scheme was proposed to enhance image encryption techniques based on a logistics algorithm Haar wavelet transform was used to distribute the image and decorrelate its pixels into averaging and differencing components. In this technique, logistic algorithm was used to encrypt the original image. While, the differencing components were compressed using a wavelet transform. The results of the proposed algorithm produced a good and reliable encryption algorithm suitable for real-time image encryption and transmission.

In this paper, a filter bank and addition Mod 2^8 with XOR is used as an image ciphering scheme, in order to enhance the security level and quality of the encrypted images. The paper is organized as follows. Section 2 presents a background of the main parameters that are usually used to assess and analyze image encryption schemes. In section 3, the proposed image encryption scheme is introduced. Section 4 introduces the experimental results and discussion. Section 5 concludes the paper.

2. INVESTIGATION OF SECURITY ANALYSIS PARAMETERS

There is a need for some performance parameters that have to be defined to evaluate and assess any given image encryption scheme. These parameters are discussed in this section.

2.1 Histogram Parameter

It is essential to ensure that encrypted and original images do not have any statistical similarities in order to avoid the outflow of information to attackers. The histogram analysis displays how pixels in an image are distributed. This can be achieved by plotting the number of pixels at each intensity level either for color or gray scale images [21]. The histogram of original image has large sharp goes up then sharply goes down while the histogram of the encrypted image contains uniform distribution which is considerably different from original image [22]. Therefore, the encrypted image histogram should be different from plaintext image histogram [23].

2.2 Entropy Parameter

Entropy is a factor that measures the ambiguity and randomness in a given information or data. For an image, the encryption should reduce the mutual data amongst pixel values and therefore increase the entropy value [24]. A good secure system should satisfy and meet a condition on the information entropy that is the encrypted image should not provide any information about the original image. The entropy value can be obtained using the following equation [25]:

$$H(m)=\sum_{i=0}^{2^N-1}p(m_i)\log_2[\frac{1}{p(m_i)}]\text{...} \quad (1)$$

where p(mi) is the probability of occurrence of the symbol mi.

Using equation (1), the ideal value of the entropy is equal 8 assuming that each symbol has equal probability of occurrence and symbols are represented 8-bits each. For a good image encryption algorithm, the entropy value should be very close to the ideal value in order to prevent entropy attack [26].

A block entropy test is sometimes required for more image ciphering analysis in order to provide qualitative and quantitative measures. In this test, the image is divided into B blocks and the entropy is determined for every block (HB) using equation (1) instead of the entropy for the entire image. Hereafter, the mean entropy of the B block entropies is calculated using equation (2) [27]:

$$\overline{H_B}=\sum_{j=0}^{B}\frac{H_j}{B}\text{...} \quad (2)$$

2.3 Correlation Coefficient Parameter

Correlation is one of the main parameters that measure the relationship between two variables to determine how much they are similar. Correlation has values in the range of -1 to +1, where 0 shows no correlation and either -1 or +1 indicates high correlation. If the correlation coefficient equals zero, then the encrypted image and the original image are completely different which means that the encryption image has no features and independent on the original image. If the correlation coefficient equal -1 or +1, this leads that the encrypted image is a negative or positive of the original image, respectively [28].

In the original image, each pixel is greatly correlated with its contiguous pixels [29]. A perfect encryption scheme should generate the encrypted-images with no such correlation in the neighboring pixels. To study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations, the following equation is used [30]:

$$r_{xy}=\frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i-E(y))^2}.}\text{...}(3)$$

In equation (3), rxy is the correlation coefficient, x and y are the values of two pixels in the same location in the original and encrypted images, respectively, E[.] is the expectation operator of the given pixel values and NxN is the image dimension.

2.4 Diffusion Characteristics

Diffusion is an essential parameter for any ciphering system. Diffusion involves that if any change in the plaintext or the key, this will directly change the ciphertext as well. One bit change in the plaintext image will lead to a significant change in the ciphered image. This is also known as the Avalanche Effect which causes a 50% change in the encrypted image due to a one bit change in the plaintext image. To measure the avalanche effect Mean Square Error (MSE) is commonly used as given in equation (4) [31]:

$$MSE = \frac{1}{MxN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j) - K(i,j)\right]^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

where I and K are two ciphertext images with keys differ by one bit. M and N are the dimensions of the images. i and j are pixel positions within the images.

To investigate the difference between the original image and the encrypted one, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are usually used. The NCPR calculates the percentage of different pixels between the original and the ciphered images. This can be obtained using equation (5) [32]:

$$NCPR = \frac{\sum_{i,j} D(i,j)}{MxN} x100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5)$$

where D(i,j) is “0” if both images have the same pixel intensities and “1” if they are different.

UACI provides the number of averaged changed intensity between ciphered images. UACI is determined by equation (6) [32]:

$$UACI = \frac{1}{MxN}\left[\sum_{i,j}\left[\frac{\left[I(i,j) - K(i,j)\right]}{255}\right]\right] x\ 100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

where I, K, M, N, i, and j are as defined in equation (4).

2.5 Key Space Parameter

For an image encryption scheme to be efficient, the key space must be large in order that any attack to be avoided. Additionally, the encryption system should be sensitive to small changes on the security keys. In a good cryptosystem, a wrong decrypted image is produced if there is a small difference in the encryption key. Therefore, an effective image encryption scheme has to be sensitive to resist any change in the keys [33].

There are two ways to test the keys used in encryption process: Key Sensitivity and Exhaustive Key Search. Key sensitivity is necessary for cipher systems. This means that the ciphered image cannot be decrypted correctly in spite of there is a minor change in ciphering and deciphering keys. This will make it secure against brute-force attacks [34]. In the cryptosystem, the key sensitivity is determined by a parameter of sensitivity of the diffusion function. The higher the parameter sensitivity value, the higher the encryption key sensitivity is. Exhaustive Key Search: A cryptosystem must possess a large key space in order to reduce the probability of the attacks on the encryption design. If a designed security system has n-bit key, the exhaustive key requires 2n attempts to discover the key. Based on this, if n is 256 bit, then 2256 trials are needed to get the correct key [35].

3. FILTER BANK WITH ADDITION MODULO 2^8 AND XOR COMBINATION FOR IMAGE ENCRYPTION

In this paper, the filter bank system is used to perform the permutation process, while the *XOR* and addition *Mod* 2^8 is used to perform the substitution process for image encryption [12]. So, the analysis filter bank is employed for image encryption and the synthesis filter bank is employed for image decryption. In this case, the encryption and decryption processes are based on linear circular convolution, which introduces a good permutation layer to achieve the diffusion. To add the required nonlinearity to the cipher to satisfy the confusion principle, *XOR* and addition *Mod* 2^8 is used as shown in Figure 1. To ensure perfect reconstruction during the decryption process, *XOR* and subtraction *Mod* 2^8 is used as shown in Figure 2, where

$\boxed{+}$: The operation of integer Addition mod 2^8, $\oplus$: The operation of exclusive-or (*XOR*),

$\boxed{<<<}$: A left rotation and $\boxed{-}$: The operation of integer subtraction mod 2^n.

This combination between *XOR* and addition *Mod* 2^8 and the filter bank provide a strong Substitution – Permutation – Network (SPN). The encryption and decryption process are shown in Figure 3 and Figure 4 for one round cipher, respectively [12]. The image encryption and decryption analysis are performed using one and two rounds of the cipher to examine the security of the image at each stage.

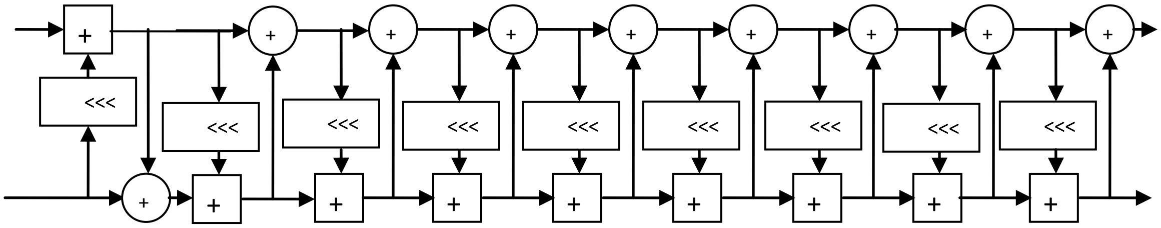

FIGURE 1: Addition *mod* 2^8 and *XOR* Combination.

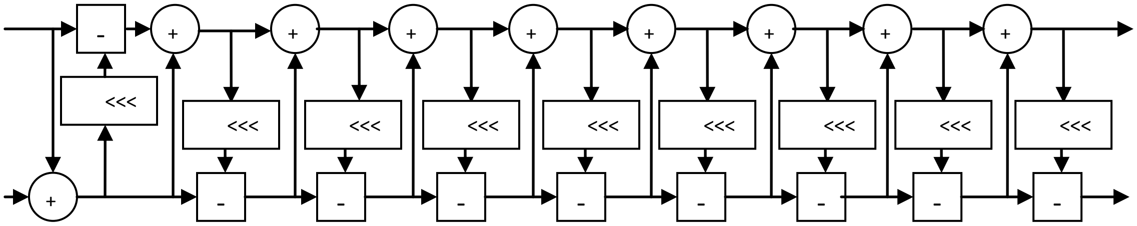

FIGURE 2: Subtraction *mod* 2^8 and *XOR* Reconstruction.

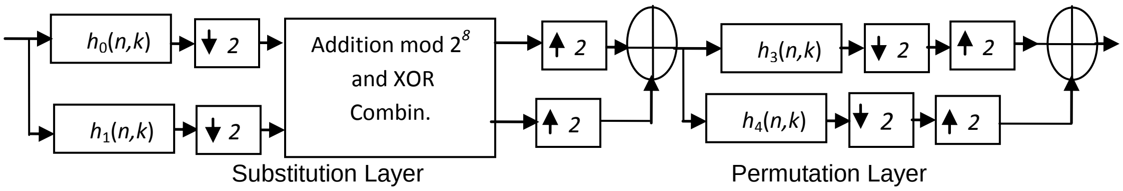

FIGURE 3: One Round for Filter Bank Encryption System.

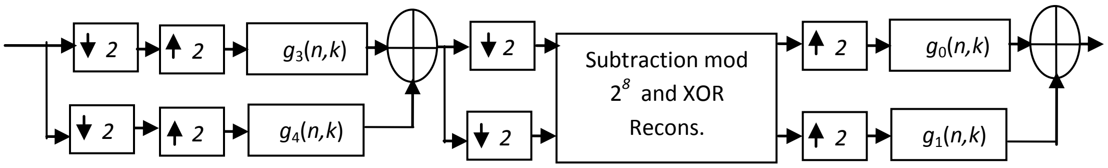

FIGURE 4: One Round for Filter bank Decryption System.

Basically, this cipher has many advantages [12]. Design simplicity, since its implementation based on digital filter design, which offers a high speed implementation in software and hardware. Also, it offers a high security level using small number of rounds. Moreover and the most important, it can introduce the scalability to the system, as it can deal with different length of key or plaintext which can be adjusted according to a particular encryption application.

4. SIMULATION RESULTS AND SECURITY ANALYSIS

In this section the security of the image encryption scheme will be evaluated for one and two round filter bank system using many parameters.

4.1 Histogram Analysis

To improve the security of the encrypted image, it is essential to ensure that, there is no statistical similarity between the original and encrypted images. The histogram is used to clarify the image pixels distribution. In this paper, the histograms for two images (Cameraman and Baboon images) and their encrypted images with one and two rounds are analysed as shown in Figure 5 and Figure 6. Note that, the histograms for the original images are not uniformly distributed, rather than, contain large sharp rises followed by sharp declines. While the histogram distributions for the encrypted images are uniformly distributed, and significantly different from the histograms of the original images. So there are no statistical similarity between the encrypted images and the original images. As a result, the encrypted images are random-like.

4.2 Information Entropy

The global entropy is employed to express the uncertainties of the system. The global information entropy for truly random gray scale source is 8. Therefore, the global entropy of the encrypted image should be very close to 8 bits to ensure its security. To study the global entropy attack, two images are encrypted using one and two rounds with different keys. Then the global entropies are calculated using equation (1) and the results are summarized in Table 1. The results in Table 1 are very closed to the theoretical value (8 bit), which means that, the information leakage in the encryption scheme is negligible, so it is secure against the entropy attack.

	Baboon Image		**Cameraman Image**	
Key	One Round	Two Rounds	One Round	Two Rounds
Key One	7.9937	7.9971	7.9931	7.9975
Key Two	7.9936	7.9975	7.9934	7.9973

TABLE 1: Global Entropy Results for Encrypted Baboon and Cameraman Images.

Another entropy attack called block entropy can be used to measure the local entropy over image blocks. To calculate the block entropies for the encrypted images, a randomly 100 non-overlapping blocks from the encrypted images have been selected. After that, the entropy for each block is calculated and recorded and averaged to find the block entropy using equation (2). The calculated values the block entropies are summarized in Table 2. It is clear that, the block entropies of the encrypted images with different keys are higher than the minimum theoretical critical block entropy for one and two rounds cipher. So, the encrypted images become random-like after encryption process.

	Baboon Image		**Cameraman Image**	
Key	One Round	Two Rounds	One Round	Two Rounds
Key One	7.1743	7.1898	7.1805	7.1907
Key Two	7.1798	7.1909	7.1735	7.1888

TABLE 2: Block Entropy Results for Encrypted Baboon and Cameraman Images.

4.3 Correlation Coefficients Analysis

To measure the relationship between the original and the encrypted images, the correlation coefficient can be utilized. It determines the encryption quality. The maximum value for the correlation coefficient is one; in this case the two variables are the same. So the correlation coefficient should be vey closed to zero to get a good encryption quality. For image encryption analysis, the correlation coefficient can be calculated between the adjacent pixels in three directions (horizontal, vertical and diagonal). This test has been carried out for Cameraman and Baboon and their encrypted images of size 256 x 256 pixels. In this test, 1000 pairs of the two adjacent pixels are randomly selected in all three directions from the images. Then, the correlation coefficients are calculated using equation (3). The results in Table 3 indicate that, after the encryption process, the highly correlated images are completely broken in all directions. Note that, before encryption, the horizontal correlation coefficient for Cameraman image is 0.9282, but after encryption using one round it becomes 0.0139, and 0.0021 after two rounds. So, the highly correlated horizontally adjacent pixels before encryption become uncorrelated after the encryption process. The same results are obtained in diagonal and vertical directions as mentioned in Table 3. Accordingly, the encryption quality is good.

	Original Images		**Encrypted Baboon Image**		**Encrypted Cameraman Image**	
Correlation Coefficients	Baboon Image	Cameraman Image	One Round	Two Rounds	One Round	Two Rounds
Horizontal	0.7103	0.9282	0.0256	-0.0062	0.0139	0.0021
Vertical	0.5966	0.9644	0.0341	0.0076	-0.0561	0.0215
Diagonal	0.6225	0.9116	-0.0239	0.0087	0.0141	-0.0040

TABLE 3: Correlation Coefficients Results.

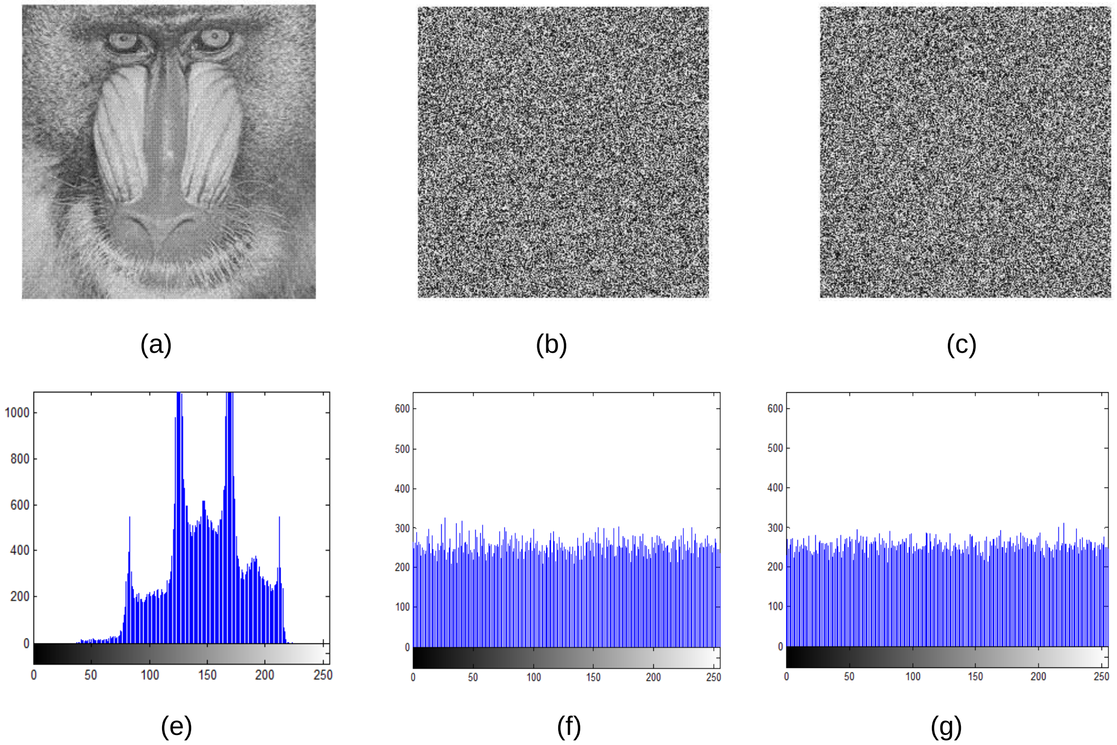

FIGURE 5: (a) Original Banoon image. (b) Encrypted image using one round. (c) Encrypted image using two rounds. (d) Histogram of the Baboon image. (e) Histogram of encrypted image using one round. (f) Histogram of encrypted image using two rounds.

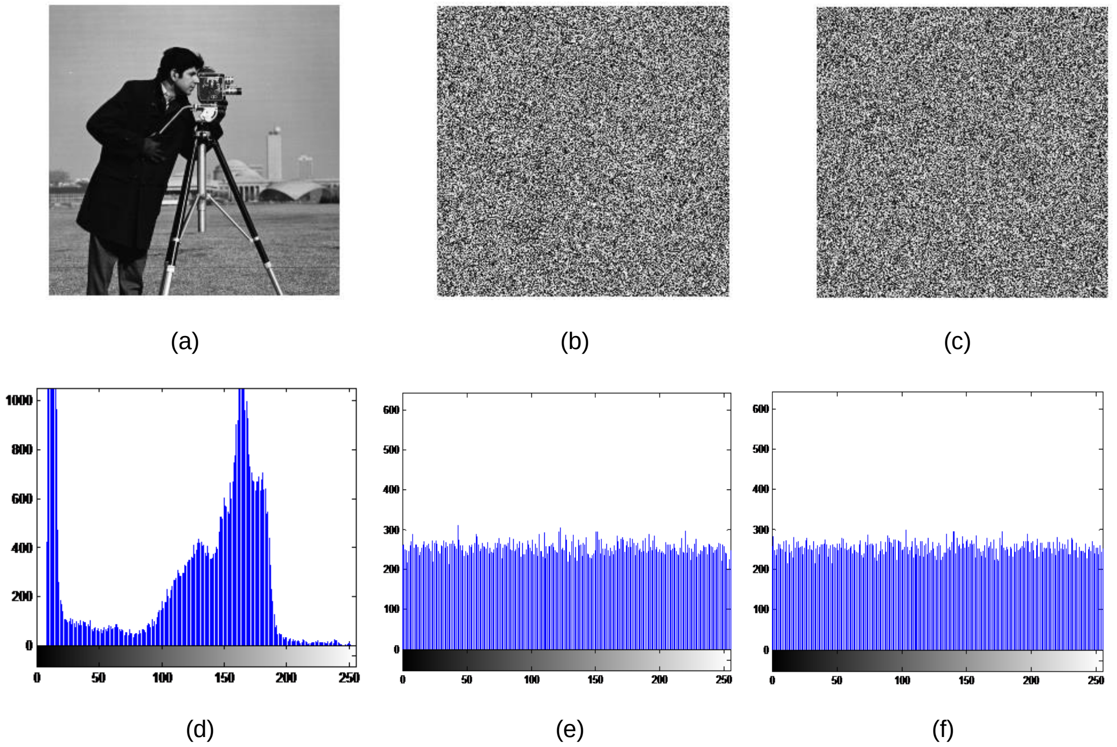

FIGURE 6: (a) Original Cameraman image. (b) Encrypted image using one round. (c) Encrypted image using two rounds. (d) Histogram of the Cameraman image. (e) Histogram of encrypted image using one round. (f) Histogram of encrypted image using two rounds.

4.4 Diffusion Characteristics

4.4.1 Avalanche Effect

The avalanche test examines the security of the encrypted image based on a small change of the original image (usually one bit differ) using the same key. To ensure the security, any small change in the original image should give a significant change in the encrypted image. In this paper, two images have been encrypted using the same key. After that, the original images with one bit differ for each has been encrypted with the same key. To check the influence of one bit change in the original images, the MSE is calculated using equation (4). The results in Table 4 ensure that, the MSE > 30 dB [36] using one or two rounds, this means, a slight difference in the original images yields a huge change to the encrypted images which certifies the diffusion principle.

Encrypted Image	One Round	Two Rounds
Baboon Image	40.11 dB	40.36 dB
Cameraman Image	40.14 dB	40.35 dB

TABLE 4: MSE Results.

4.4.2 NPCR and UACI

To examine the security of the image encryption scheme against the differential attack, NPCR and UACI can be employed. NPCR measures percentage of the number of different pixel to the total number of pixels. UACI computes the average intensity of the differences between the images. So to examine the influence of one bit change, these tests are performed on Baboon and Cameraman images. Simulation results obtained in Table 5 show that, the encryption scheme using number different of rounds is very sensitive to a small change in the original images. Note that, the higher the value of NPCR and UACI, the better the encryption scheme. As a result a strong diffusion has been done, and the encrypted images are very random- like. Then the efficiency of the differential attack is vanished and practically useless.

Encrypted Image	One Round NPCR	Two Rounds NPCR	One Round UACI	Two Rounds UACI
Baboon Image	99.55	99.67	33.38	33.61
Cameraman Image	99.59	99.66	33.35	33.60

TABLE 5: NPCR and UACI Results.

4.5 Key Space Analysis

A strong image encryption scheme must be very sensitive to the key. To evaluate the key space analysis two methods are used.

4.5.1 Exhaustive Key Analysis

Basically the proposed cipher is a scalable cipher, so it can deal with different key length based on the required security level. In this paper the minimum key length images is 128 bit. So, if an attacker uses 1000 MIPS computer to break the key using the brute force attack, the attacker needs

$$\frac{2^{128}}{1000\times10^{6}\times60\times60\times24\times365} > 10.79\times10^{21} \text{ Years}$$

This is very long time period which is infeasible [30].

4.5.2 Key Sensitivity Test

To test the sensitivity of the encrypted decrypted image due to a minor change of the key, key sensitivity test can be used. The key sensitivity can be addressed with respect to two portions:

1) Encryption: if the same image (P) is encrypted using key 1 (K1) and key 2 (K2) which are different in one bit only. Then how is the difference between the two encrypted images (C1 and C2).

2) Decryption: if the encrypted image (C1) is decrypted using two encryption keys (K1 and K2), which are different only in one bit. Then how is the difference between the two decrypted images (D1 and D2).

Suppose that, there are three keys (K1, K2 and K3) where all differ only in one bit. Then, the encryption process has been performed for the images (Baboon and Cameraman) using one and two rounds. Figures 7 and 8 show the sensitivity of the encrypted and decrypted images using one or two rounds due to the small change of the key. As a result, the confusion property is satisfied over the encrypted images using both one and two rounds. The corresponding percentage differences between two encrypted images with one bit differ in the key for Baboon and Cameraman images are calculated as depicted in Table 6.

Encrypted Image	One Round	Two Rounds
Baboon Image	99.5850%	99.6560%
Cameraman Image	99.5770%	99.6600%

TABLE 6: Difference of When Keys Differ by One Bit Results.

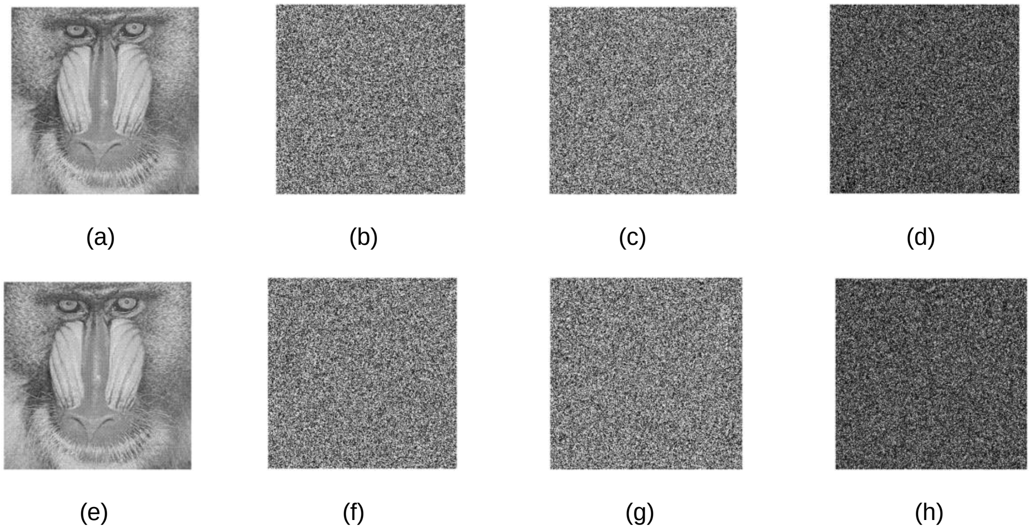

FIGURE 7: (a) Original Baboon image (P). (b) Encrypted image using K1 with one round (C1). (c) Encrypted image using K2 with one round (C2). (d) Encrypted images difference |C1 – C2|. (e) Decrypted image (C1) using K1 gives (D1). (f) Decrypted image (C1) using K2 gives (D2). (g) Decrypted image (C1) using K3 gives (D3). (h) Decrypted images difference |D2 – D3|.

4.6 Statistical Comparative Evaluation Results

To evaluate the security of image encryption using two rounds filter bank cipher, it is important to compare it with other popular image encryption ciphers. In this paper, the simulation results for two rounds cipher are compared with two image encryption schemes; namely, AES and Compression Friendly Encryption Scheme (CFES) which were analyzed in [21]. The values in Table 7 demonstrate that, the two rounds of the proposed filter bank cipher is stronger than

CFES; in addition it has the same results as AES and some results better than the AES results. Moreover, the filter bank cipher supports simpler implementation and scalability, where the other ciphers do not provide the scalability.

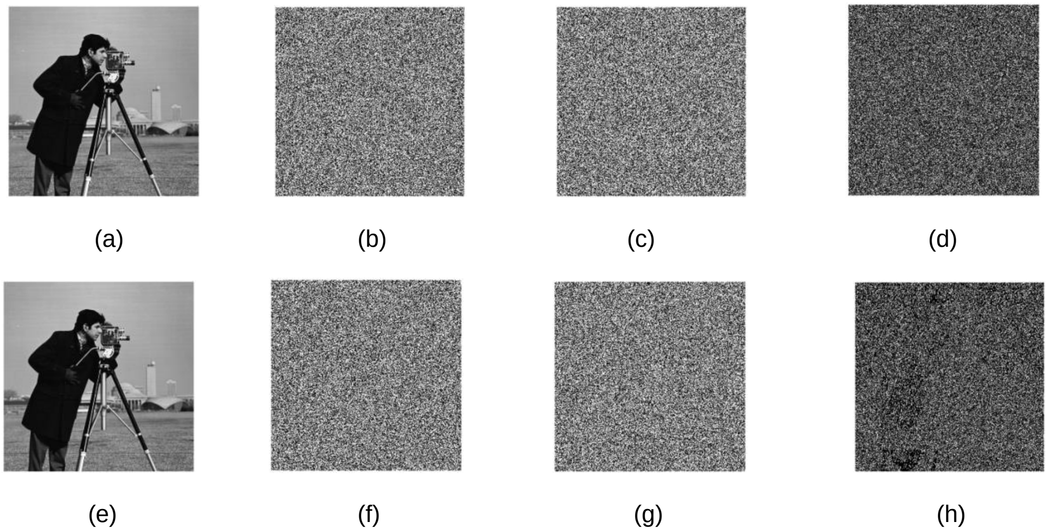

FIGURE 8: (a) Original Cameraman image (P). (b) Encrypted image using K1 with two rounds (C1). (c) Encrypted image using K2 with two rounds (C2). (d) Encrypted images difference |C1 – C2|. (e) Decrypted image (C1) using K1 gives (D1). (f) Decrypted image (C1) using K2 gives (D2). (g) Decrypted image (C1) using K3 gives (D3). (h) Decrypted images difference |D2 – D3|.

	Encrypted Baboon Image			**Encrypted Cameraman Image**		
	AES	**CFES**	**Proposed**	**AES**	**CFES**	**Proposed**
Horizontal Correlation Coefficient	-0.0370	0.9547	-0.0062	-0.0067	0.9522	-0.0021
Vertical Correlation Coefficient	0.0107	0.0611	0.0076	0.0504	0.0124	0.0215
Diagonal Correlation Coefficient	-0.0419	-0.0025	0.0087	-0.0156	0.0202	0.0040
Global Entropy	7.9973	7.1404	7.9975	7.9975	7.1455	7.9975
Block Entropy	-	-	7.1909	-	-	7.1907
NPCR	99.62	99.09	99.67	99.60	99.12	99.66
UACI	33.36	15.39	33.61	33.53	15.49	33.60
MSE	40.34 dB	33.31 dB	40.36 dB	40.39 dB	33.86 dB	40.35 dB
Key Sensitivity	99.6506%	99.1882%	99.6560%	99.5880%	99.2554%	99.6600%

TABLE 7: Parameters Evaluation Comparison with AES and CFES.

5. CONCLUSIONS AND FUTURE WORK

In this paper, the image encryption quality using filter bank with XOR and addition *Mod* 2^8 combination cipher with one and two rounds are evaluated and analyzed using many evaluation parameters. The evaluation parameters are histogram analysis, correlation coefficient, global entropy, block entropy, avalanche effect, NPCR, UACI, exhaustive key analysis, and key sensitivity test. The overall results proved the security of the proposed algorithm. The simulation results for histogram showed that the distribution of the encrypted image is uniform and completely different from the histogram of the original image. In correlation coefficient analysis, the correlated adjacent pixels of the original images are completely distributed in the encrypted image with very small correlation coefficient in all directions (horizontal, vertical and diagonal), so the highly correlated images are uncorrelated after encryption. The global and block entropy are very close to ideal, so the encrypted image represent random – like image. The diffusion characteristics for the encryption scheme were proved through avalanche test, NPCR and UACI. The key sensitivity results showed that image encryption and decryption are very sensitive to any minor change in the key. Accordingly, the image encryption process passes all these tests; as a result, the encryption process is considered as a strong and robust process to resist many existing cryptography attacks and cryptanalysis technique. Also, the results obtained in this paper are compared with other image cipher schemes; the proposed cipher shows it's leading. To ensure the image encryption security and immunity against cryptanalysis technique, it is better to use two rounds filter bank with *XOR* and addition *Mod* 2^8 combination cipher even the result for one round showed good security. In future work, the performance analysis for audio and video signal will be evaluated and investigated using the proposed cipher.

6. REFERENCES

[1] F. BORKO, S. DANIEL, and M AHMET.Fundamentals of multimedia encryption techniques. Multimedia Security Handbook, 2004.

[2] H. AHMED, H. M KALASH, and O. S FARAG ALLAH.: Encryption analysis of the rc5 block cipher algorithm for digital images. Menoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt 2006.

[3] H. RATHOD, M. SISODIA, and S SHARMA." A review and comparative study of block based symmetric transformation algorithm for image encryption." International Journal of Computer Technology and Electronics Engineering (IJCTEE) 1(2), 2011.

[4] N. FERGUSON, B. SCHNEIER, and A KOHNO. Cryptography engineering. 2nd edition, John Wiley & Sons, 2010.

[5] A. GUPTA, N. JOSHI and C. NAGAR, "A review new symmetric image encryption scheme based on correlation pattern." International Journal on Emerging Technologies 3(1): 2012, pp 102-104.

[6] K. MILOZŠ, "Qualitative aspects of image applications in multimedia technology." 17th IEEE International Conference on Radioelektronika, April 2007, Prague, pp.1 – 11.

[7] B. FURHT and D. KIROVSKI. Multimedia security handbook. CRC Press, Boca Raton, Florida, 2005.

[8] P. KARTHIGAIKUMAR and S. RASHEED. "Simulation of image encryption using AES algorithm." IJCA Special Issue on Computational Science - New Dimensions & Perspective 2011.

[9] M. A. BANI YOUNES and A. JANTAN. "Image encryption using block-based transformation algorithm." IAENG International Journal of Computer Science, 35(1) 2008a.

[10] M. A. BANI YOUNES and A. JANTAN "An image encryption approach using a combination of permutation technique followed by encryption." International Journal of Computer Science and Network Security (IJCSNS), 8(4) 2008b.

[11] S. H. KAMALI, R. SHAKERIAN, M. HEDAYATI, and M. RAHMANI. "A new modified version of advanced encryption standard (aes) based algorithm for image encryption." IEEE Transactions on Electronics and Information Engineering, 2010a, 1:141-145.

[12] S. SARAIREH and M. BENAISSA. "A scalable block cipher design using filter banks over finite fields." In Acoustics Speech and Signal Processing (ICASSP), IEEE International Conference, Dallas, TX, USA 2010.

[13] S. H. KAMALI, R. SHAKERIAN, M. HEDAYATI, and M. RAHMANI. "A new modified version of advance encryption standard based algorithm for image encryption." International Conference in Electronics and Information Engineering (ICEIE) 2010b.

[14] B.V. RAMA DEVI. "A novel encryption method for the secure transmission of images." International Journal on Computer Science and Engineering, 2(9): 2010, pp 2801-2804.

[15] H. XIAO and G. ZHANG. "An image encryption scheme based on chaotic systems." IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian 2006.

[16] Y. ZHANG. "Image encryption using extended chaotic sequences." IEEE Transactions International Conference on Intelligent Computation Technology and Automation, 2011a pp: 143-146.

[17] Y. ZHANG. "Image encryption with logistic map and cheat image." 3rd International Conference on Computer Research and Development (ICCRD), 2011b, 1: 97 – 101.

[18] L. KRIKOR, S. BABA, T. ARIF and Z. SHAABAN. "Image encryption using DCT and stream cipher." European Journal of Scientific, 32(1) 2009, pp47-57.

[19] Z. ZHOU SHIHUA, Z. QIANG, and W. XIAO-PENG. "Image encryption algorithm based on DNA sequences for the big image." International Conference on Multimedia Information Networking and Security, 2010, pp 884-888.

[20] N. SETHI and D. SHARMA. " A new cryptology approach for image encryption." 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), 2012, pp 905 – 908.

[21] J. AHMAD and F. AHMED. "Efficiency analysis and security evaluation of image encryption schemes." International Journal of Video and Image Processing and Network Security, 12(4), 2012.

[22] A. JOLFAEI and A. MIRGHADRI. "Image Encryption Approach Using Chaos and Stream Cipher." Journal of Theoretical and Applied Information Technology, 2010a.

[23] A. JOLFAEI and A. MIRGHADRI. "Survey: image encryption using A5/1 and W7." Journal of Computing, 2(8), 2010b .

[24] S. E. BORUJENI, and M. ESHGHI. "Chaotic image encryption design using tompkins-paige algorithm." Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 762652, 2009.

[25] U. PANDEY, M. MANORIA, and J. JAIN. "A novel approach for image encryption by new m box encryption algorithm using block based transformation along with shuffle operation." International Journal of Computer Applications, 42(1), 2012.

[26] R. ENAYATIFAR. "Image Encryption Via logistic map function and heap tree." International Journal of Physics Science, 6(2) 2011.

[27] S. RAKESH, A. AJITKUMAR, B. SHADAKSHARI, and B. ANNAPPA. "Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping." International Journal on Cryptography and Information Security (IJCIS), 2(1) 2012.

[28] B. AÏSSA, D. NADIB, and R. MOHAMED. "Image encryption using stream cipher based on nonlinear combination generator with enhanced security." NEW TRENDS IN MATHEMATICAL SCIENCES, 1(1) 2013, pp 18-27.

[29] A. N. PISARCHIK and M. ZANIN. "Image encryption with chaotically coupled chaotic maps." Physica D, 237(20): 2008 pp 2638-2648.

[30] I. ELASHRY, O. ALLAH, A. ABBAS, S. RABAIE, and F. EL-SAMIE. "Homomorphic image encryption." Journal of Electronic Imaging, 18, 2009.

[31] Z. HEGUI, L. XIAOJUN, T. QINGSONG, Z. XIANGDE, and Z. CHENG. "A new chaos-based image encryption scheme using quadratic residue." IEEE International Conference on Systems and Informatics (ICSAI), 2012, pp 1800-1804.

[32] C. K. HUANG, and H. H. NIEN. "Multi chaotic systems based pixel shuffle for image encryption." Optical communications, 282, 2009, pp 2123-2127.

[33] A. DIACONU, and K. LOUKHAOUKH. "An improved secure image encryption algorithm based on rubik's cube principle and digital chaotic cipher." Mathematical Problems in Engineering, Hindawi Publishing Corporation, 2013.

[34] S. LIAN, J. SUN, and Z. WANG. "Security analysis of a chaos-based image encryption algorithm." Physics Letters A 35, 1, 2005, pp 645-661.

[35] A. M. RIAD, A. H. HUSSEIN, H. M. KASEM, and A. ABOU EL-AZM. "A new efficient image encryption technique based on arnold and idea algorithms." International Conference on Image and Information Processing (ICIIP 2012), 46, 2012, Singapore.

[36] Z. LIEHUANG, L. WENZHUO, L. LEJIAN, and L. HONG. "A novel image scrambling algorithm for digital watermarking based on chaotic sequences." International Journal of Computer Science and Network Security, 6(8B), 2006, pp 125–130.