SECURITY ANALYSIS OF FBDK BLOCK CIPHER FOR DIGITAL IMAGES

M. Kiran Reddy[1], K. J. Jegadish Kumar[2]

[1]M.E-Communication Systems, [2]Assistant Professor, Electronics and Communication Department, SSN College of Engineering, Tamilnadu, India

Abstract

Network security is one of the major concerns in the modern world. In this regard, a strong security technique is required to protect user data. Cryptography techniques plays an important role in secured transmission through encryption of data and thus ensuring integrity, authenticity, confidentiality of information. Several encryption algorithms have been proposed like AES (Advanced Encryption Standard), DES (Data Encryption Standard) and RSA. These provide very good encryption for text applications. However, these encryption schemes appear not to be ideal for image applications. Some algorithms like GKSBC and RC6 provide very good encryption for digital images. New techniques are emerging that are aimed at providing secured transmission of images over networks. The FBDK (Fixed Block with Dynamic Key Size) block cipher is a new cryptography technique designed using simple operations like XOR, substitutions, circular shifting. The FBDK algorithm is applicable for blocks of any size with key size being dynamic for each block. It does not involve any complex mathematical operations like modular exponentiation. It is a hybrid cryptography technique based on symmetric key and asymmetric key cryptosystems. This paper investigates the security of FBDK block cipher for digital images against brute-force attack, statistical analysis and Differential analysis attacks. In this paper, various security analysis tests has been discussed which are helpful in finding out whether the FBDK encryption algorithm can do secure encryption or not. Experimental results proves the security and efficiency of FBDK cipher for images against all aforementioned types of attacks which justifies its consideration for real time image applications.

Keywords: *Cryptography, Ciphers, Encryption, Security, and cryptanalysis.*

----------***----------

1. INTRODUCTION

The security of digital images is more important since the communication of digital products over open networks occur more and more frequently. Special and efficient technique is needed for storage and transmission of data securely. Encryption is the most practical security technique for digital data in computer systems.

In order to fulfill such a task, many encryption methods have been proposed such as DES, AES and RSA. However, these encryption schemes appear not to be ideal for image applications, due to bulk data capacity and high redundancy. Also, they involve complex mathematical calculations that require more time. In [2], FBDK block cipher was proposed, which is capable of handling any block size with dynamic key size based on the size of the message. The design procedure of the FBDK algorithm is given in detail in [2]. This paper explores the security of FBDK algorithm regarding brute force, statistical attacks and Differential analysis in secured transmission of digital images. The experiments carried out along with their outcomes are discussed in detail in the following sections.

2. SECURITY ANALYSIS AND TEST RESULTS

A good encryption technique has thoroughly rearranged pixel positions, values transformed and visually transformed processes. Some security analysis parameters [1] which are done on FBDK algorithm are:

1. Statistical analysis
2. Key space analysis
3. Encryption quality
4. Differential analysis

2.1 Statistical Analysis

Shannon introduced two methods known as diffusion and confusion which will make intruders and their attackers more bewildered [1]. Diffusion means spreading out the influence of a single plain image pixel over many cipher image pixels. Confusion means, using transformations that Complicate the dependence of statistics of the cipher image on the statistics of the plain image [1]. The statistical analysis test is done by finding out histogram and correlation of encrypted image with respect to original image. The tests were performed using Microsoft Windows 2008 on Intel(R) core(TM) i3-2350 CPU, 2.3 GHz to 2 GB of RAM using Matlab 7.0.

2.1.1 Histogram

These are the first visual test performed by the intruders as well as sender and receiver while decryption [1]. The histogram of original and encrypted image must totally be different, so that no sort of information about the original image can be obtained from the encrypted image. Figure 1 shows the histograms of the original image "Cameraman.tif" and its encrypted image. From the figure 1 it can be seen that the histogram of encrypted image is completely different from that of the original image and hence the FBDK algorithm is highly resistant to histogram analysis and intruder can gain no information from the encrypted image through visual tests.

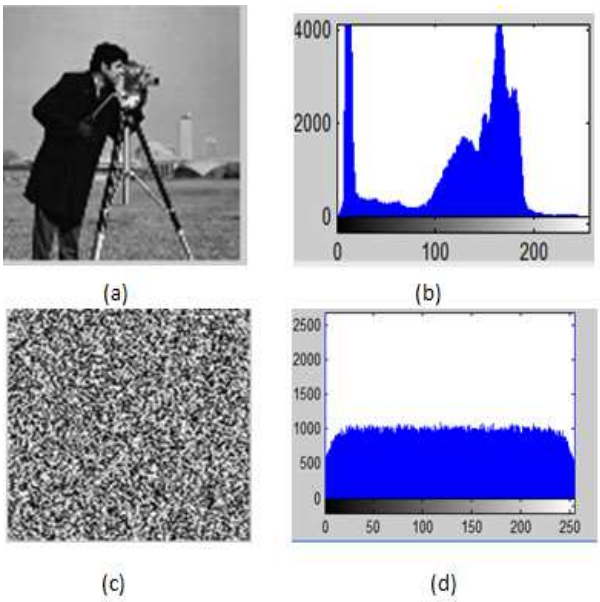

Fig -1: Histogram analysis using FBDK algorithm. (a) Original Image, (b) Histogram of Original Image, (c) Encrypted Image, (d) Histogram of Encrypted Image.

2.1.2 Correlation Coefficient

Correlation coefficient gives the degree of similarity or relationship between original and encrypted images [7]. Let A be the original image and B be the encrypted image of size MXN. Then the correlation coefficient denoted by ϒ is calculated as,

$$\Upsilon = \frac{\sum_m \sum_n (A_{mn} - A_m)(B_{mn} - B_m)}{\sqrt{(\sum_m \sum_n (A_{mn} - A_m)^2)(\sum_m \sum_n (B_{mn} - B_m)^2)}}$$

Where, A_{mn} is pixel intensity at m^{th} row and n^{th} column of original image, B_{mn} is pixel intensity at m^{th} row and n^{th} column of encrypted image. A_m is mean of all elements in original image A and B_m is mean of all elements in encrypted image B. The table 1 shows the correlation coefficient values obtained for various images encrypted using FBDK algorithm.

Table -1: Correlation coefficient of standard Images encrypted with FBDK algorithm

Image	Size	ϒ
Singer.jpg	256X256	-0.0005
Lena.tif	512X512	-0.0022
Pirage.tif	512X512	0.0006

The range of ϒ is -1 to +1. If the correlation coefficient value is close to -1 or +1 then the original and encrypted images are highly correlated and a significant information about original image can be easily obtained from encrypted image. If ϒ is close to zero then the original image and encrypted image are highly uncorrelated and this implies the encryption efficiency is high. From Table 1 the ϒ values obtained by encrypting various standard images are very low (nearly zero) which indicates that the original image and encrypted image are highly uncorrelated and hence statistical attacks using correlation is very difficult. The results of Histogram analysis and Correlation coefficient tests prove that the FBDK algorithm is highly resistant to statistical attacks. In the next section, the algorithm's resistance to key space analysis is investigated.

2.2 Key Space Analysis

The key space refers to the number of bits used to encrypt image. The key size should be large enough to tackle key space analysis also known as brute force search attack. Here, all possible key combinations are tried on the encrypted message. Suppose, if the original key length used by the receiver is of N bits, then 2^N combinations of key are possible. If the N is very large, then it will be very difficult for the attacker to try all the combinations. In the worse case, the minimum number of searches the intruder must perform in order to get the original key should be $2^{N/2}$. The security of an algorithm depends on its resistance to brute force search. The proposed algorithm is analyzed against brute force search and the experimental results prove it to be more resistant to key space analysis. The table 1 shows the brute force search time required with different N values and at an average decryption time of 2.456. In the proposed algorithm the key length varies for each block and hence it is very difficult for the attacker to know the key length and to perform key analysis. Since, the text and image data is highly encrypted and there is no pattern of input seen in the encrypted output, the proposed algorithm is also resistant to traffic analysis and release of message content attacks.

Table -2: Brute Force search analysis of FBDK algorithm

Key Length (in bits)	Brute Force search time (years)
128	5.61e+36
136	5.28e+38
144	1.29e+41
152	3.36e+43

The table 2 shows that if a key of length 128 bits is used then the time required to perform brute for search is 5.61e+36 years. This is very large when compared with the lifetime of the message that is being transmitted. Hence proposed algorithm is highly resistant to brute force search attack or key space analysis.

2.3 Encryption Quality

A good encryption scheme must posses high encryption quality and low execution time [7]. In this section, encryption quality and performance analysis tests were conducted on FBDK algorithm using text and image files. The tests were performed using Microsoft Windows 2008 on Intel(R) core(TM) i3-2350 CPU, 2.3 GHz to 2 GB of RAM using Matlab 7.0.

2.3.1 Encryption Analysis

To determine the encryption quality two tests Viz., EQ measure, and PSNR (Peak Signal to Noise Ratio) value calculation is performed.

2.3.1.1 Encryption Quality (EQ) measure

When an image is encrypted there will be a change in its grey scale values. The EQ [7] measure gives the amount of deviation of grey scale values in original and encrypted images. Let I denote the original image and I' denote the encrypted image each of size M*N pixels with L grey levels. Let HL(I) denote the number of occurrences of each grey level L in the original image and HL(I') denote the number of occurrences of each grey level L in the encrypted image. The encryption quality [7] represents the average number of changes to each grey level L and is expressed mathematically as,

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} \left| H_L(I') - H_L(I) \right|}{256}$$

The table 3 gives a comparison between GKSBC and FBDK in terms of EQ. All the images are of size 512X512 and FBDK has high EQ values compared to GKSBC [7]. Hence, the proposed algorithm proves to be efficient for image encryption when compared with GKSBC.

Table -3: EQ comparison between GKSBC and FBDK

Image File	EQ (GKSBC)	EQ (FBDK)
Lena (512X512)	663.82	714.65
Baboon (512X512)	773.90	823.71
Girl (512X512)	894.89	939.71

2.3.1.2 PSNR Value

An efficient encryption algorithm produces an unintelligible image [3] as output. The parameter that can be used for determining the encryption efficiency of the algorithm is the PSNR (peak signal to noise ratio) [4] value in decibels (dB). Ideally, PSNR value between the actual image and encrypted image (PSNR_A_E) should be 0 dB and between the actual image and decrypted image (PSNR_A_D) it should be infinity [7]. Practically an efficient algorithm give a PSNR value less than 9 dB between actual image and encrypted image, a PSNR value between (30-60) dB between actual image and decrypted image. Table 2 shows the PSNR values obtained with various standard test images taken as input to the proposed algorithm. For all the images the PSNR value is quite good, this also indicates that the algorithm can tolerate various statistical attacks like the traffic analysis, autocorrelation analysis etc. The PSNR values for decrypted image show that the original image can be reconstructed efficiently from the encrypted image.

Table -4: PSNR values for different Standard test images encrypted using FBDK

Image name	Dimensions	PSNR_A_E (dB)	PSNR_A_D (dB)
Cameraman.tif	256 X 256	8.389	37.8532
Singer.jpg	225 X 225 X 3	8.6653	46.9137
Pirate.tif	512 X 512	8.9183	36.6502

2.4 Differential Analysis

Generally, the intruder tries to make slight changes such as modifying one pixel of the encrypted image, and then observes the change of the result. After such changes, if the attacker is able to obtain any relevant information about original image from the encrypted image then the algorithm used for encryption is practically inefficient. Also, the encrypted image must be sensitive to small changes in original image. If a change in original image can cause a significant change in the cipher image with respect to diffusion and confusion, then the differential attack becomes very inefficient on that image. The methods [1] used to study the influence of one-pixel change on the whole image, encrypted by FBDK are: Number of Pixels Change Rate (NPCR) and Unified Average changing Intensity (UACI). NPCR gives the number of pixels change rate in encrypted image when one pixel

change occurs in original image [1]. Consider two encrypted images T1 and T2, whose original images have only one pixel difference. Then, NPCR of two images is defined as [1]:

$$\text{NPCR} = \frac{\sum_{i,j} S(i,j)}{w*v} * 100\%$$

$$\text{Where, } S(i,j) = \begin{cases} 0, & \text{if } T_1(i,j) = T_2(i,j) \\ 1, & \text{if } T_1(i,j) \neq T_2(i,j) \end{cases}$$

w=number of rows in an image, v=number of columns in an image, (i,j)=Position of Pixels

Another method, UACI is unified average changing intensity which measures the average intensity of differences between original image and ciphered image [1]. The formula for UACI is:

$$\text{UACI} = \frac{1}{w*v} \sum_{i,j} \frac{(T_1(i,j) - T_2(i,j)}{255} * 100\%$$

NPCR or UACI are random variables dependent on parameters such as the image size and format of image rather than statistical values. For UACI the typical value taken on an average for different image sizes is 34% and for NPCR score the upper bound is 100% (ideal value) which indicates, it is difficult to establish relationship between the images. One performed test is on the one-pixel change influence on a 256 grey-scale image "cameraman.tif" of size 256X256. The Figure 2 (b) shows the encrypted image and figure 2 (c) shows the encrypted image obtained after one pixel value in the original image is changed. The NPCR and UACI values for different image sizes are listed in Table 5.

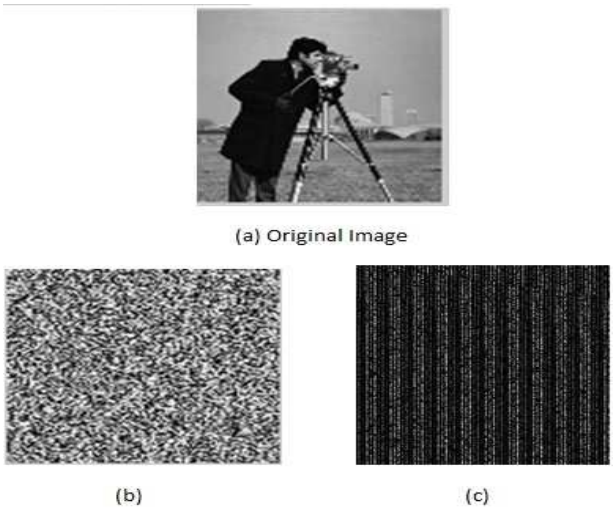

Fig -2: (a) Original Image, (b) Encrypted Image, (c) Encrypted Image after pixel value change.

The encrypted images before and after pixel change are completely scrambled. There is no significant information about the original image is available in these images. From table 5, we can find the values of NPCR and UACI to be very close to ideal value for all size of images. This indicates that no sort of relationship can be established between the encrypted images.

Table 5 NPCR and UACI values for images of different sizes encrypted with FBDK

Size	NPCR	UACI
128X128	99.2432%	33.254%
256X256	99.2523%	33.384%
512X512	99.3147%	33.462%

The NPCR and UACI tests prove that the FBDK algorithm is resistant to differential analysis and hence it can be used efficiently for digital image encryption for secured transmission through the communication networks. Also, the clearance of the differential analysis tests indicates that the algorithm is also resistant to attacks like chosen plaintext, chosen ciphertext, traffic analysis.

3. CONCLUSIONS

In modern communication world, image encryption plays a crucial role, and hence, an efficient encryption algorithm is necessary. The paper provides encryption efficiency analysis and security evaluation of FBDK algorithm. The various security analysis tests shows that FBDK block cipher can be considered to be a real-time encryption technique for digital images.

ACKNOWLEDGEMENTS

The authors wish to express heartful thanks to the faculty of ECE, SSN College of Engineering, Chennai for their support to this research.

REFERENCES

[1]. Taranjit Kaur, Reecha Sharma, "Security Definite parameters for image encryption techniques", International journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 5, May, 2013.

[2]. M.Kiran Reddy and K.J.Jegadish Kumar, "Implementation of Novel Hybrid Cryptography Algorithm", In press.

[3]. M. Ashwak AL-Abiachi, Faudziah Ahmad, Ku Ruhana, " A Competitive Study of Cryptography Techniques over block cipher", UKSim 13th International Conference on Modelling and Simulation, 2011.

[4]. Amitesh Singh Rajput, Nishchol Mishra, Sanjeev Sharma, "Towards the Growth of Image Encryption and Authentication Schemes", International Conference on Advances in

Computing, Communicactions and Informatics (ICACCI), 2013.
[5]. G. Chen, Y. Mao and C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos Solitons Fractals 2004; 21:749-61, 2004.
[6]. Nitty Sarah Alex and L. Jani Anbarasi, "Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography", IEEE International Conference on ICASSP, 1985.
[7]. S. Arul jothi and M. Venkatesulu, "Encryption Quality and Performance analysis of GKSBC algorithm", Journnal of Information Engineering and Applications, vol 2, No.10, 2012.

BIOGRAPHIES

M.Kiran Reddy is currently pursuing his Masters degree in communication systems in SSN Collegeof Engineering,
Email-id: kiran.reddy889@gmail.com

K.J.Jegadish Kumar is working as Assistant Professor in SSN college of Engineering, Chennai in ECE Department.
Email-id: jegadishkj@ssn.edu.in