ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 1, Issue 3

Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)

Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma

Abstract: - The primary goal of this paper is security management. This will provide authentication of users, and integrity, accuracy and safety of images which is traveling over internet. Moreover, an image-based data requires more effort during encryption and decryption. The Proposed Architecture for encryption and decryption of an image using suitable user-defined key is developed with the same objective. In this paper, we introduce a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image we will binary value blocks, which will be rearrange into a permuted image using a permutation process, and then the generated image will be encrypted using the "Hyper Image Encryption Algorithm (HIEA)" algorithm.

Key Word: - Encryption, Decryption, Cryptography, Image Encryption

I. Introduction

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. From the study of research paper and other I have conclude that in [10, 11, and 12] there are no clarifications which type of images they are using to perform image encryption and decryption procedure. I have also analyzed that there is no clarification about the configuration of machine and platform where all the experiment are calculating. Another thing which I have measured that proposed transformation table of [10, 11, and 12] have very complex structure and not easy to understand which is the cause of poor efficiency. From further study I have observed that Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data.

The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the Characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

After the detailed study of image encryption, we presented some problem which find during study and how we can remove these with the help of our proposed work. This paper is divided in to four sections. Section – I basic introduction about image encryption and problem formulation, section-II detailed description of proposed work, section-III experiment and results comparison and section-IV conclusion and future enhancement.

II. Proposed Work

A. *Proposed Architecture*: proposed architecture is shown in figure 1.

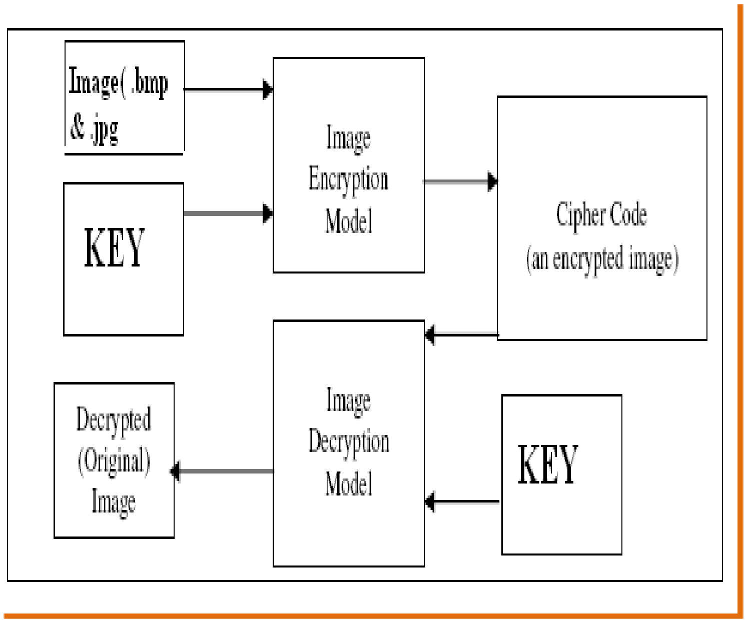


Figure 1:- Proposed Architecture

Comparatively Architecture of various algorithms with my Proposed Architecture: Figure 2 is showing comparative study architecture between various algorithm and proposed algorithm

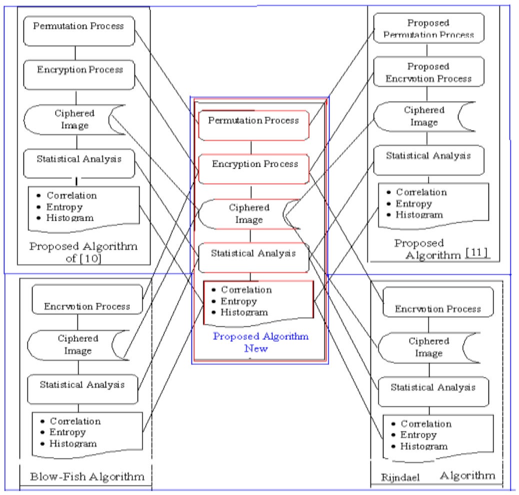


Figure 2:- Block Diagram of Proposed Technique versus Various Techniques

B. Graphical Representation:-

Initially in proposed image encryption system requires .bmp or jpeg type of image file that is to be hidden. It has two modules encrypt and decrypt shown in figure 3. Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. Here I used some .net tool in this software called "Image Crypto System (ICS)" that is written in VB.Net language and we can use this software to hide our visual information in .bmp or jpeg type of pictures.

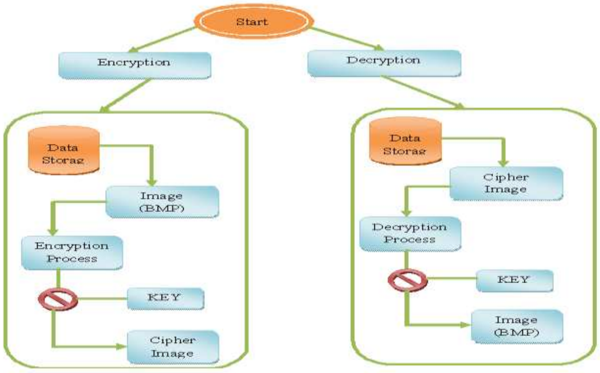


Figure 3:- The graphical representation of Image Encryption system

The encrypt module is used to hide visual information like bmp or jpeg image; no one can see that visual information in bmp file or jpeg files. This module requires bmp or jpeg type of image message and gives the only one image file in destination.

The decrypt module is used to get the hidden visual information in original image. It take the cipher image file as an output, and give one file at destination folder, is that bmp or jpeg image file.

C. Proposed Algorithm for Creating Transformation Table:-

1: Select Image to be encryption from data store
2: Insert key of 256 bits
3: Calculate Image Pixels Value
    Horizontal Value of Pixel = PixelWidth/10
    Vertical Value of Pixel = PixelHeight/10
4: Select a Random Function to Calculate Final value for Horizontal and Vertical Pixels
    HorizontalPixel → Select Random Value between Horizontal Value of Pixel and PixelWidth
    VerticalPixel → Select Random Value between Vertical Value of Pixel and PixelHeight
5: Select a Variable No-Of-Pixel to store Multiple Value of HorizontalPixel and VerticalPixel
    No-Of-Pixel = HorizontalPixel X VerticalPixel
6: Using Hash Function (Here I am using SHA-1) I am generating a Seed Value. This SHA-1 will apply on 256 bits Selected Key
    Seed = SHA-1(Above Selected KEY)
7: Divide Seed into two Part equally Seed-1 and Seed-2
    Seed-1 → First Half of Seed
    Seed-2→ Second Half of Seed
8: If Seed-1 is Greater Then Seed-2 Then We Will Select another Variable SeedValue and assign any numeric value between 0 to 4 (Randomly Chooseable) Otherwise Value of SeedValue Variable vary between 5 to 9 (Randomly chooseable).
9: If Variable SeedValue is Equal Between 0 to 4 then calculate new seed value (Here we are working on ASCII value of seed).
    Seed = Seed + (Seed-1 Mod 2) + 1
    Otherwise
    Seed = Seed + (Seed-2 Mod 2) + 1
10: Repeat Process 8 to 9 till No-Of-Pixel/2
11: Final Output of Step 10 will represent Create transformation Table
12: Exit

Steps for Proposed Encryption Algorithm:

1: Select an Image which is having at least 256 bits in Size to be encryption.

2: Calculate Binary Value of Image.

3: Select First 256 bits form Binary Value and create 16 sub blocks of 16 bits. This process will repeat till end of file.

4: Select Key Value of 256 bits. And create 16 sub blocks of 16 bits.

5: Select 64 bits from transformation table. And create 4 blocks of 16 bits.

6: Apply Logical operation XOR between first 8 block of selected image and second 8 block of selected key. Result will stored in image blocks of

7: Apply Logical operation XOR between last 4 blocks of selected images and 4 blocks of transformation table. Result will store in image blocks.

8: Apply Circular Shift Operation on last 4 block of selected key and second last 4 block of selected image.

9: Apply logical XOR operation between selected image and key which is output of step 8. Result will store in image block.

10: Apply Circular Shift Operation on 4 blocks of transformation table and second last 4 block of selected key.

11: Apply logical XOR operation between transformation t table and selected key, which is output of step 10. Result will store in key block.

12: Combine output of step 6, 7, 9, and 11 in such that it should be produced 256 bits total.

13: output of step 12 will become input for next round.

14: Repeat step-1 to step-13, 10 times.

15: After 10th round, cipher text will produce of selected image.

16: Exit.

D. Characteristics of an Image Cryptosystem:-

For studying characteristics of image encryption, we must first analyze the implementing differences between image and text data:

1. When cipher text is produced, the decrypted text must be equal to the original text in a full lossless manner. However, this requirement is not necessary for image; the cipher image can be decrypted to an original image in some lossy manner.

2. Text data is a sequence of words, it can be encrypted directly by using block or stream ciphers. However, digital image data are represented as 2D array.

3. Since the storage space of a picture is very large, it is inefficient to encrypt or decrypt image directly. One of the best methods is to only encrypt/decrypt information that is used by image compression for reducing both its storage space and transmission time.

In general, there are three basic characteristics in the information field: privacy, integrity and availability. For privacy, an unauthorized user can not disclose a message.

For integrity, an unauthorized user cannot modify or corrupt a message. For availability, message is made available to authorized users faithfully. A perfect image cryptosystem is not only flexible in the security mechanism, but also has high overall secure performance, the image security requires following characteristics:

1. The encryption system should be computationally secure. It requires an extremely long time to attack, unauthorized user should not be able to read privileged image.

2. Encryption and decryption should be fast enough not to grade system performance. The algorithm for encryption and decryption must be simple enough to be done by user in personal computer.

3. The security mechanism must be as widespread as possible.

4. The security mechanism should be flexible.

5. There should not be a large expansion of encrypted image data.

III. Experiments

In this paper .Net implementation is used to present an evaluation system. For entropy calculation and execution time of the known image encryption algorithm with my proposed image encryption algorithm, it is necessary to describe the detailed evaluation method, as illustrated in Figure-4. Here I am taking only one evaluating modes to find whether the key and the images have impact on time consuming of image cryptographic algorithms: DISK (different images in the same key).

.

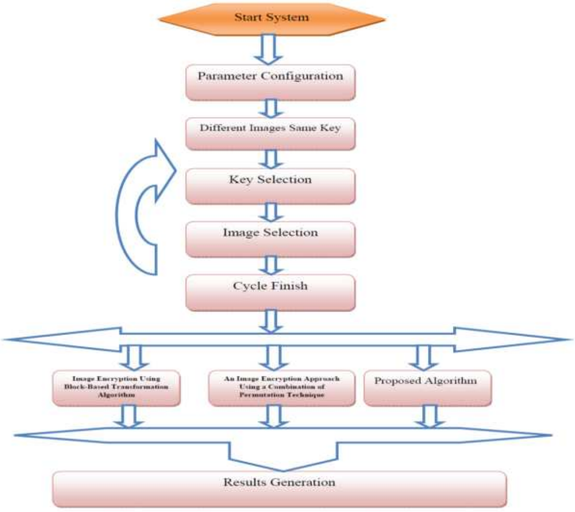

Start System
Parameter Configuration
Different Images Same Key
Key Selection
Image Selection
Cycle Finish
Image Encryption Using Block-Based Transformation Algorithm
An Image Encryption Approach Using a Combination of Permutation Technique
Proposed Algorithm
Results Generation

Figure 4: Results Evolution Model

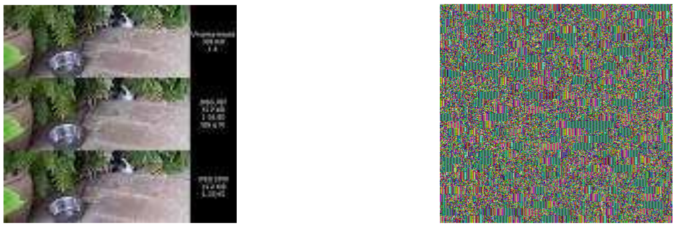
For our experiment, we use a laptop Pentium® Dual-Core CPU T4400 @2.20Ghz and 32-bit Operating System, The algorithm was applied on a Joint picture Expert Group (JPEG) image that has the size of 300 pixels x 300pixels with 256 colors. In order to evaluate the impact of the number of blocks on entropy,and here entropy is calculate by using following equation Entropy defined as follows [14]-[15]

$$\boldsymbol{He} = -\sum_{K=0}^{G-1} \boldsymbol{P(K)}\ \mathbf{log\,2(\,P(K\,))}\ldots\ldots\ldots\ \mathbf{(1)}$$

Where:
He: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol *k*.

In the experiments, the laptop encrypts an images data and calculates entropy and encryption time. We are using some parameters for entropy one is numeric value and second is percentage ratio which is shown in Table 1. Here I am also calculating execution time which is shown in Table-2

I do n cycles (that is, the number of the evaluated images). In each cycle, four same type images are respectively encrypted by "Image Encryption Using Block-Based Transformation Algorithm", "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" and "Proposed Algorithm (PA)" by copying them. Finally, the outputs of the evaluation system are entropy and execution time, and measured in numeric form. Actually, for an encryption algorithm, the entropy not only depends on the algorithm's complexity, but also the key and the images have certain impact. The image is decomposed into 10 pixels × 10 pixels blocks. Figure 5.shows the resulted images.



(a) **(b)**

Figure 5. Results of encryption by using 10 pixels × 10 pixels blocks. (a) Original image. (b) Encrypted image using proposed algorithm

Result Comparison in Tabular Form: - In this I am going to represent our result in the form of table. After comparison the results that were obtained can be well represented in form of Table 1-5 that describes the encryption time, decryption time, entropy of original image, entropy on encrypted image and security setting in the above discussed algorithms. And also calculate performance of CPU utilization and memory utilization.

Images(Size in KB)	Image Encryption Using Block-Based Transformation Algorithm	An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption	Proposed Algorithm
D:\heeral\image\2.jpeg (3.59)	0:00:03	0:00:09	0:00:03
D:\heeral\image\3.jpg (3.48)	0:00:03	0:00:09	0:00:03
D:\heeral\image\4.jpg (3.09)	0:00:03	0:00:09	0:00:03
D:\heeral\image\5.jpg (4.33)	0:00:04	0:00:12	0:00:04

Table-1:- Encryption Time Comparison of various Image Encryption Algorithm with Proposed Algorithm

Images(Size in KB)	Image Encryption Using Block-Based Transformation Algorithm	An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption	Proposed Algorithm
D:\heeral\image\2.jpeg (3.59)	0:00:03	0:00:09	0:00:03
D:\heeral\image\3.jpg (3.48)	0:00:03	0:00:09	0:00:03
D:\heeral\image\4.jpg (3.09)	0:00:03	0:00:09	0:00:03
D:\heeral\image\5.jpg (4.33)	0:00:04	0:00:12	0:00:04

Table-2:- Decryption Time comparison of various Image encryption Algorithm With proposed Algorithm

Images(Size in KB)	Image Encryption Using Block-Based Transformation Algorithm	An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption	Proposed Algorithm
D:\heeral\image\2.jpeg (3.59)	15.509775	15.509775	15.509775
D:\heeral\image\3.jpg (3.48)	49	56	68
D:\heeral\image\4.jpg (3.09)	14	14	14
D:\heeral\image\5.jpg (4.33)	25	42	28

Table-3:- Entropy of Original Image Comparison of various Algorithm with Proposed Algorithm

Images(Size in KB)	Image Encryption Using Block-Based Transformation Algorithm	An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption	Proposed Algorithm
D:\heeral\image\2.jpeg (3.59)	139281.1296	1460846.781	15739907.4
D:\heeral\image\3.jpg (3.48)	110558.6174	1080029.519	52672743.39
D:\heeral\image\4.jpg (3.09)	168641.228	2271031.568	19838321.82
D:\heeral\image\5.jpg (4.33)	246469.9004	4185951.26	75427376.8

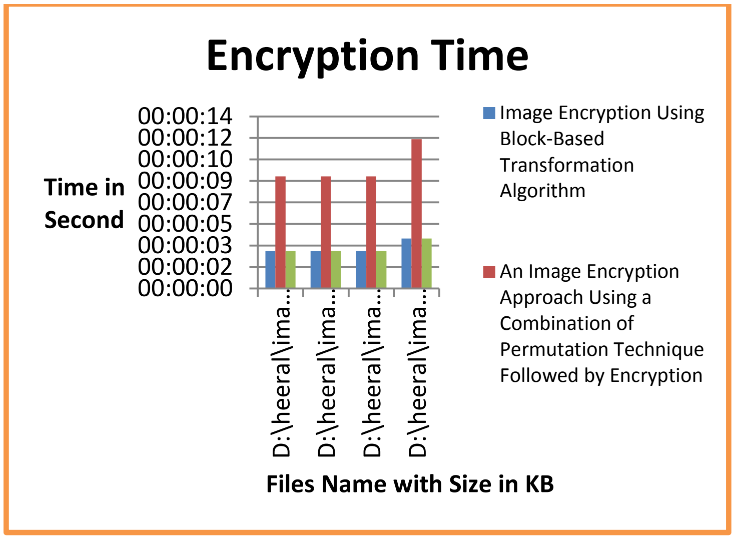
Table-4:- Entropy of Encrypted Image Comparison of various Algorithm with Proposed Algorithm

Algorithms	CPU Utilization at Encryption in %	CPU Utilization at Decryption in %	Memory Utilization in %
Image Encryption Using Block-Based Transformation Algorithm	25	50	-25
Image Encryption Approach Usinga Combination ofPermutation Technique Followed by Encryption	31	50	-19
Proposed Algorithm	37	51	-14

Table-5:-CPU and Memory Utilization of various Algorithms with proposed Algorithm

Graphical Representation of Comparison: - In this I am going to represent our result comparisons in the form of graph.

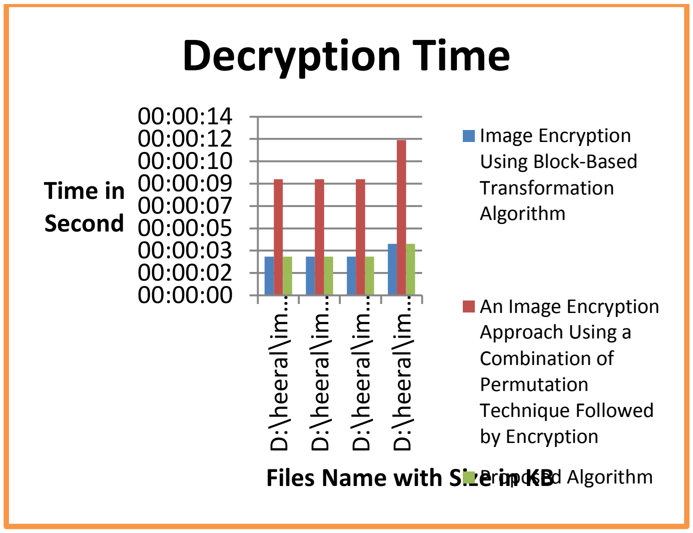
Encryption Time: Here I am drawing the Graph-1 form Table-1 to reveal it. In this graph, the evaluated mode is DISK, and the fixed size of the evaluated image. At this point, the key length of all Encryption algorithm is 256-bit, which is equals to that of the proposed algorithm (PA).



Graph 1:-:- Encryption Time Comparison of Existing Algorithm with Proposed Algorithm

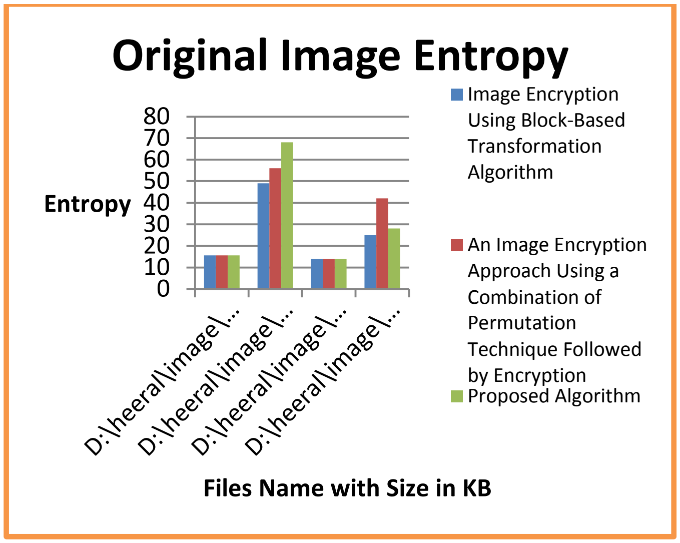
Decryption Time: Here I am drawing the Graph-2 form Table-1 to reveal it. In this graph, the evaluated mode is DISK, and the fixed size of the evaluated image.

At this point, the key length of all Encryption algorithm is 256-bit, which is equals to that of the proposed algorithm (PA).



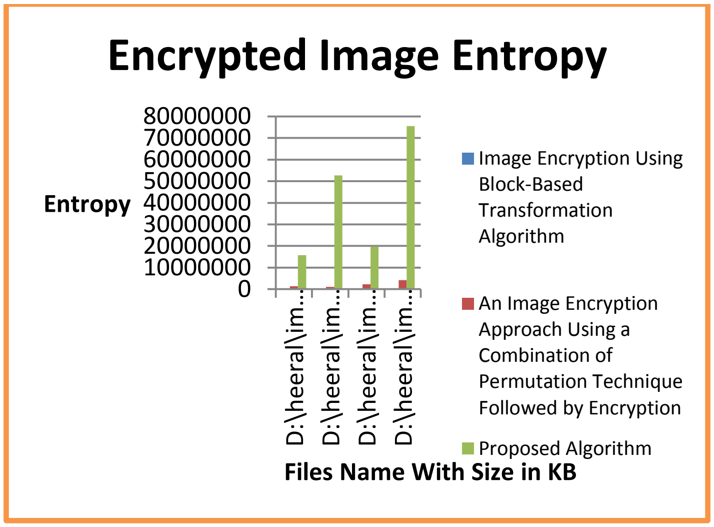
Graph 2:-:- Decryption Time Comparison of Existing Algorithm with Proposed Algorithm

Entropy of original Image: - Here I am drawing graph 3 from table 3. In this graph I am presenting entropy of original images of various encryption algorithms as well as our proposed algorithm.



Graph 3:- Entropy of Original Image Comparison of Existing Algorithm with Proposed Algorithm

Entropy of Encrypted Image: - Here graph 4 table 4. In this graph I am presenting encrypted images entropy of various encryption algorithms as well as our proposed algorithm.



Graph 4:- Entropy of Encrypted Image Comparison of Existing Algorithm with Proposed Algorithm

Experimental results for this compassion point are shown Table 1-5 at encryption stage. The results show the superiority of proposed algorithm over other algorithms in terms of the entropy, CPU utilization as well as memory utilization which are our main task of this research. Another point can be noticed here; that “Image Encryption Using Block-Based Transformation Algorithm” requires less encryption time about 4 to 5 second differences than as compare “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption algorithms”. Some typical results obtained by the evaluation system can be found in Table 5. The results illustrated in Table 5 show that our Proposed Algorithm (PA) is 70% better than other selected algorithms in DISK evaluation mode firstly. Finally, it is not difficult to find that, in contrast with those Tables, the larger the key length is, and the bigger security is. Besides, in contrast with that Table, it is not difficult to find that the increasing key length can lead to the significant increment of entropy as well as CPU utilization. Generally speaking, the entropy of cryptographic algorithm usually depends on the size of images, keys and structure of algorithm.

IV. Conclusion And Future Work

The difference of efficiency between our "Proposed Algorithm" and "Image Encryption Using Block-Based Transformation Algorithm", "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" is very high approximately 80% . If the security and efficiency is of primary concern then one can use our proposed algorithm. From the above discussion we can clearly see that the proposed algorithm has 70% better entropy of encrypted image any of the other compeering algorithms and hence can be incorporated in the process of encryption of any images. Also, we can see that the "Image Encryption Using Block-Based Transformation Algorithm" and "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" have very less entropy and hence cannot be used for encryption of confidential messages. The encryption algorithm presented above, is a very simple, direct mapping algorithm using feistal Structure and some logical operation. This cipher image generation provides a good strength to the encryption algorithm. As such it is quite essential to improve our algorithms performance in future.

References

[1] Onwutalobi Anthony-Claret "Using Encryption Technique" Department of Computer Science,University of Wollongong Australia, Anthony.claret@ieee.org

[2] Prof. Mrinmoy Ghosh and Prof. Pranam Paul "An Application to ensure Security through Bit-level Encryption" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009

[3] Fauzan Saeed and Mustafa Rashid "Integrating Classical Encryption with Modern Technique" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

[4] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud "Performance Evaluation of Symmetric Encryption

[5] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud " Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010

[6] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.

[7] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms" 2009 International Conference on Computational Intelligence and Security

[8] William stallings, "Cryptography and Network Security:Principles & Practices", second edition

[9] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005William stallings, "Cryptography and Network Security:Principles & Practices", second edition,

[10] Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm" IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03 Advance online publication: 19 February 2008.

[11] Mohammad Ali Bani Younes 1† and Aman Jantan 2 "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[12] Kamlesh Gupta1, Sanjay Silakari2 "Choase Based Image Encryption Using Block-Based Transformation Algorithm"(IJCNS) International Journal of Computer and Network Security,Vol. 1, No. 3, December 2009.

[13] S. P. Nana'vati., P. K. panigrahi. "Wavelets:applications

[14] M. Sonka, V. Hlavac. and R. Boyle, "Digital imageprocessing," in: image Processing, Analysis, and Machine Vision, 1998, 2nd ed. http://www.pws.com

[15] D. Feldman, "A brief introduction to: information theory, excess entropy and computational mechanics,"college of the atlantic 105 eden street, bar harbor, me 04609, 2002, http://hornacek.coa.edu/

Author Biography

Ms.Hiral Rathod received B.E in computer engineering from Dharmsinh Desai University in Gujarat in 2007 M.Tech pursuing from Oriental Institute of Science & Technology, Bhopal.

Mr. Mahendra Singh Sisodia received M.Tech in computer science and currently Assistant Professor in Oriental Institute of Science & Technology, Bhopal. He has 6 years teaching experience and also has published two (International Journal) and five (International Conference). His Research areas in Data Mining Network Security**.**

Mr. Sanjay Kumar Sharma Assistant Professor in Department of Computer Science & Engineering of Oriental Institute of Science & Technology, Bhopal..