AN ANALYSIS ON IMAGE ENCRYPTION FOR SECURED TRANSMISSION OF BIOMEDICAL APPLICATIONS

A.Mohanarathinam[1], N.B.Prakash[2], G.R.Hemalakshmi[3], Kamalraj Subramaniam[4], G. K. D. Prasanna Venkatesan[5]

[1]Assistant Professor, [4]Associate Professor, [5]Dean
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
[2]Associate Professor, [3]Assistant Professor (Sr.Grade),
National Engineering College, Kovilpatti, Tamil Nadu, India.

Abstract: Digital images are very popularly used for communications over the internet. Embedded information in the digital image has to be securely transmitted without any modification in the image. The biomedical telemedicine gains significant importance in information transmission and with increasing popularity with Tele-ophthalmology, requirement of medical data confidentiality and privacy also increases for data storage and secure transformation. The objective is to analyse the bioimage encryption algorithms which provides security and privacy to the bioimages. In this paper retinal fundus image online available dataset have used. The proposed work is analysed by considering, three performance parameters such as PSNR, MSE and CR. The two different encryption algorithms namely block-based perceptual encryption (BBPE) and advanced encryption standard (AES) algorithm along with arithmetic compression have tested . The proposed work results tested on standard test images and retinal fundus images shows that the BBPE method attains PSNR of 27.58db , MSE of 3.20e+03 and CR of 4.27 for standard test images and 13.35db, 1.4046e+04 and 7.28 respectively for medical HRF images. The BBPE algorithm can be used in tele-ophthalmology and telemedicine applications.

***Keywords*: Block-Based Perceptual Encryption- Image compression - Biomedical image**

1. Introduction

In the current scenario, it was understood that enormous digital based service and management has been evolved for the customers. The main concern about the usage of various digital services are security, storage, transmission and reception of digital modalities. Data Security is most needed in this digital era, because the most of the transmitted digital information are hacked by intruders easily. To transmit the digital data's and information, encryption is the preferred technique used for the protection of transmits data. Various encryption algorithms has been developed by the researchers. Image encryption algorithm based on block based transformation consisting of encryption with secret key, steganography and watermarking. This algorithm is used for the information security and it has evaluated in terms of performance parameters PSNR and MSE [1]. The encryption decryption algorithm for text and Image using Advanced Encryption Standard was developed and implemented in DSP processor [2]. AES algorithm for the effective security of data communication was designed [3] and AES algorithm was implemented using FPGA code with very high speed integrated circuit and synthesized using Xilinix ISE and ModelSim software [4]. AES algorithm with 128 bit encoder was designed [5]. A simple and fast encryption algorithm using scan patterns and XOR has been implemented for image encryption. The algorithm was implemented for various sample images and the results proved that the robustness and advantage of the algorithm [6]. A simple and secure image encryption using block based transformation algorithm was introduced. To convert Spatial domain components to frequency domain DCT was developed and DCT coefficients with higher frequencies components were encrypted [7]. AES algorithm image encryption and decryption was implemented where the encrypted cipher images displayed the uniformly distributed RGB pixels [8]. The performance of various image encryption schemes was analysed with parameters such as tenability, visual degradation, compression friendliness, speed and cryptographic security [9]. Block Based Symmetric Transformation encryption algorithm was designed [10]. Crypto system for fundus images was developed. Multiscale Approach for Blood Vessel Segmentation on Retinal Fundus Images was developed [11]. Encryption and decryption algorithms for Tele-ophthalmology was developed and was inferred that it was suitable for real time applications [12]. The vessel segmentation by matched filtering in colour retinal images was proposed [13]. Encryption-Then-Compression algorithm was developed [14]. The block based image compression and encryption was developed for secured image communication[15-17]. After having the detailed study about the encryption algorithm, we have analyzed the performance of block based perceptual encryption and the AES algorithm with arithmetic compression techniques for the bioimage.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

2. Methodology

In order to analyse the performance of BBPE and AES algorithms, the encryption algorithms have applied to standard test images and bioimages. The standard test images like Lena, Baboon, Barbara, boat and etc. have chosen from SIPI data set. The HRF database retinal fundus images have also used in our proposed work.

The two techniques implemented in this research work are listed below and the performance analysis was done based on the parameter such as PSNR, compression ratio and MSE.

- Block based perceptual encryption algorithm.
- AES encryption algorithm.

2.1 Block Based Perceptual Encryption

The block diagram of the proposed block based perceptual image encryption is shown in Figure.1

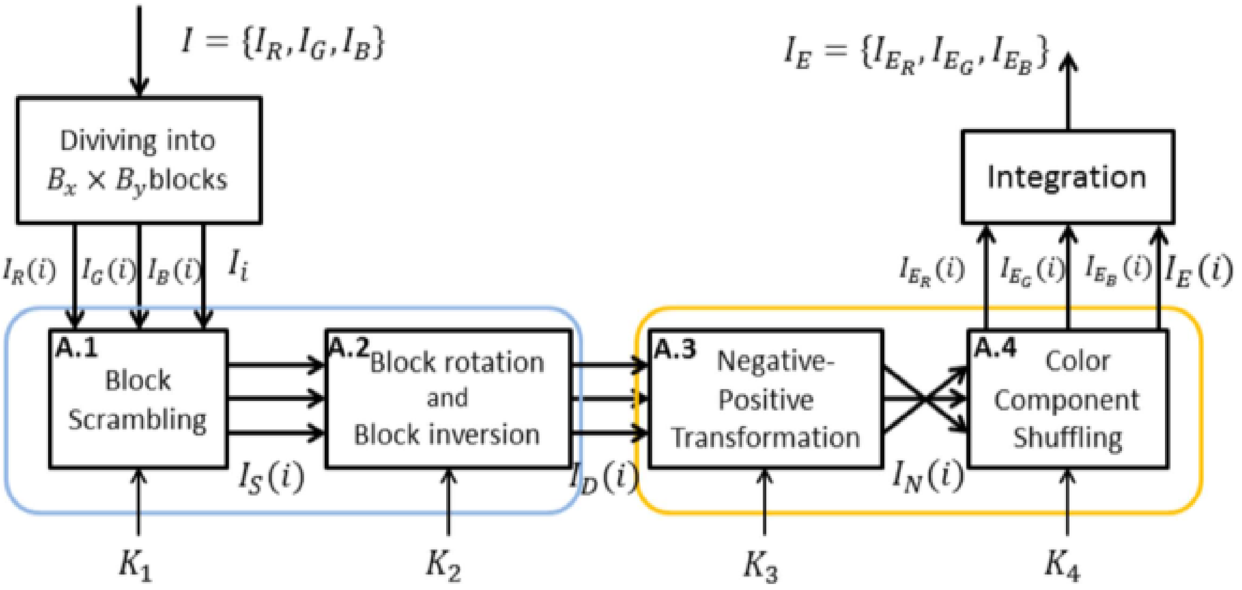


Figure.1 Block based perceptual encryption – Block Diagram

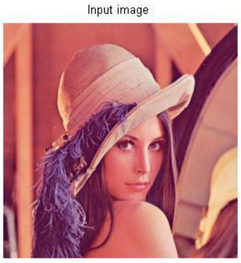
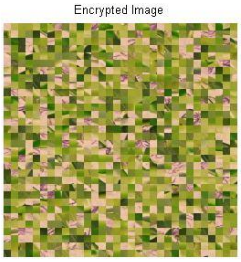
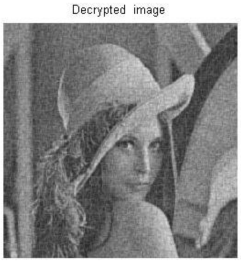
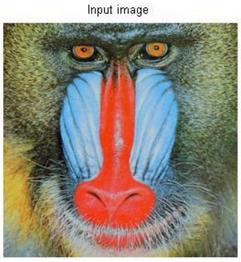
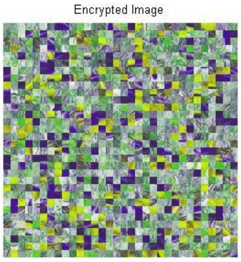
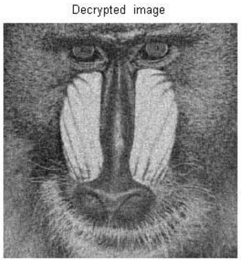
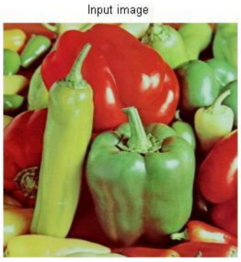
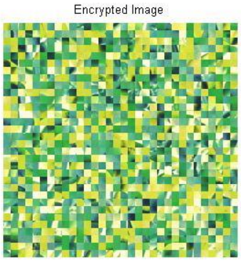
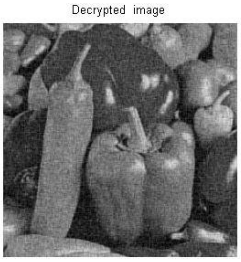
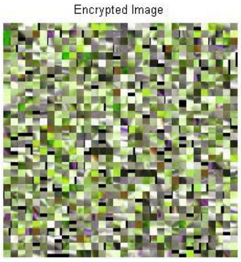
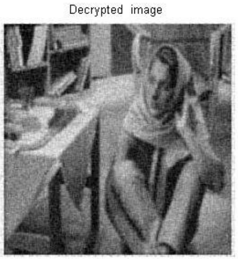
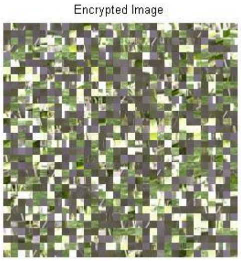
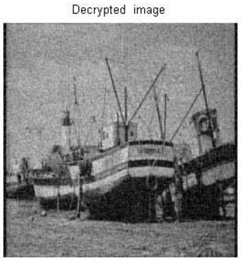
The step by step procedure of the block based perceptual encryption algorithm is explained below.

1. Divide input image into Bx X B_y blocks image.
2. Perform block Scrambling using randomly generated key K_1
3. Rotate and invert each block using key K_2
4. Transform pixel values from negative to positive using key K3
5. Shuffle color components in each block using key K_4.
6. Generate the encrypted image by integrating the transformed block images.

2.1.1 Experimental Results

The algorithm described above was implemented with MATLAB R2013a and results obtained for the standard images like Lena, Baboon, Pepper, Barbara Boat images and also HRF images are shown in Figure.2

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Lena Image			
Baboon Image			
Pepper Image			
Barbara Image			
Boat Image			

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

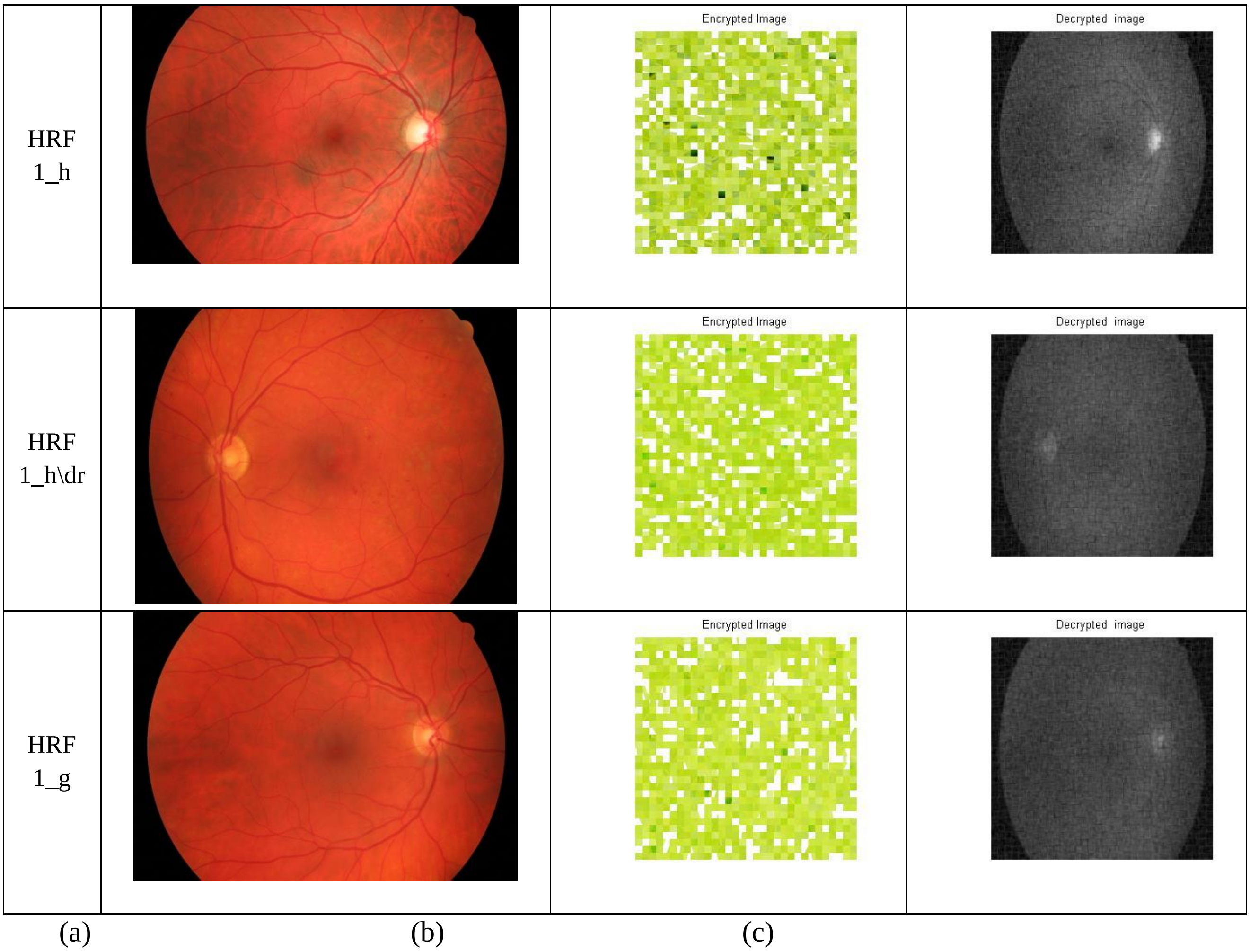


Figure.2 (a) Input image and (b) encrypted image (c) decrypted image

2.2 Advanced Encryption Standard (AES) Algorithm

AES is derived from the basic principle of a substitution-permutation network.

It gives the symmetric block cipher among 128 bits of block size and it operates on 4× 4 column-major order matrix of bytes. In AES function, the size of round key is used for cipher and it identifies the number of replications of transformation rounds that change the plain text into cipher text. Then, this output is transferred to AES encryption scheme. Each and every round has some progressing steps and each of one has four similar steps however various stages, as well as one that depends on the encryption key itself. To get the original text from cipher text, a group of reverse rounds has been carried out by using same encryption key.

The AES has following loop functions

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

The overall flow of the encryption process of AES algorithm is show in Figure.3.

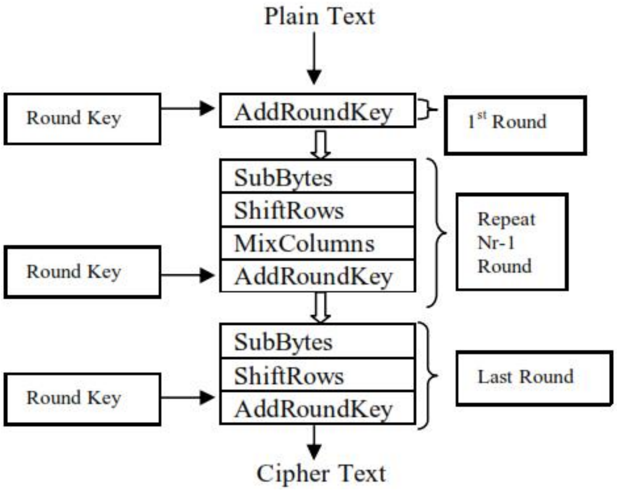


Figure.3 AES Algorithm – Block Diagram

After the completion of the AES algorithm follows the arithmetic encoding and the image decompression method where which the final output will be obtained as shown in Figure.7

2.2.1 Arithmetic Compression

Arithmetic encoding is used for lossless data compression and it works on one data symbol per iteration. The encoding algorithm depends on three parameters such as Next symbol to be encoded, current interval and probability assigned to each symbol. The encoding process involves the following procedures,

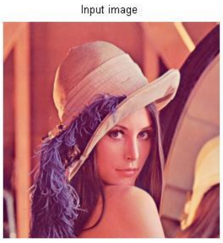
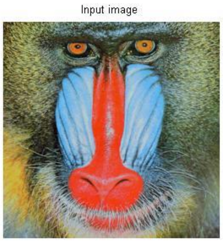
- Represent the source ensemble by an interval [0,1] initially.
- Divides the interval into sub interval.
- Interval corresponds to actual symbol to be encoded becomes interval used in the next step

This process will be repeated until all the symbols are encoded.

After completion of arithmetic compression, compression ratio is calculated using compressed image. The data compression is an essential process, while performing image communication and medical data transmission.

2.2.2 Experimental Results

The implementation of the Arithmetic Compression was done on the standard test images and also HRF images. The results obtained are shown in Figure.6.

Lena Image		
Baboon Image		

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

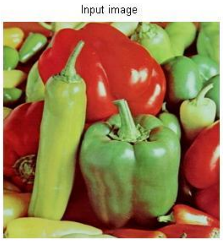
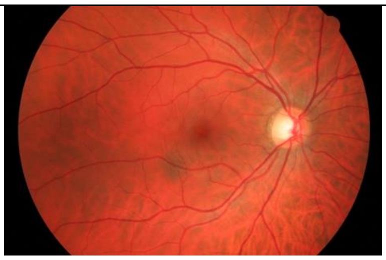
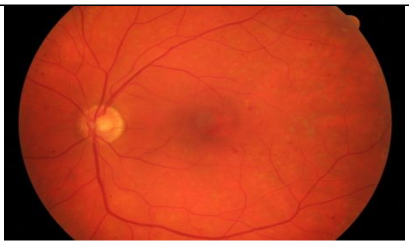
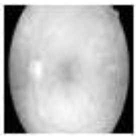
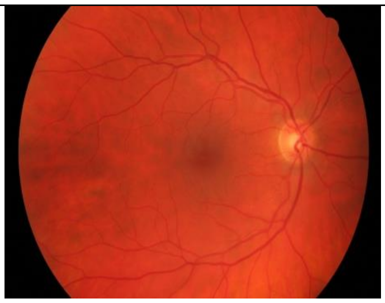
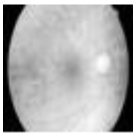
Pepper Image		
Barbara Image		
Boat Image		
HRF 1_h		
HRF 1_h\dr		
HRF 1_g		

Figure.4 AES algorithm input and resultant output images.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

3. Results and Discussion

The experimental results have been evaluated by measuring performance metrics such as PSNR, MSE and compression-ratio.

PSNR:

PSNR can be used to appraise an encryption scheme, which indicates the changes in pixel values between the actual image and the encrypted image.

$$PSNR = 10 \log 10(255^2 / MSE) \quad (1)$$

Mean Square Error (MSE):

The MSE defined as the square of error between original image and retrieved frame. The distortion in reconstructed image is calculated by using MSE

$$MSE = \frac{\sum\sum[A(i,j) - B(i,j)]^2}{N \times N} \quad (2)$$

A(i,j) – Original Image

B(i.j) – retrieved image

N × N = row and column of image intensity of pixel values range

Compression Ratio(CR):

Compression reduces storage space and transmission bandwidth is measured by,

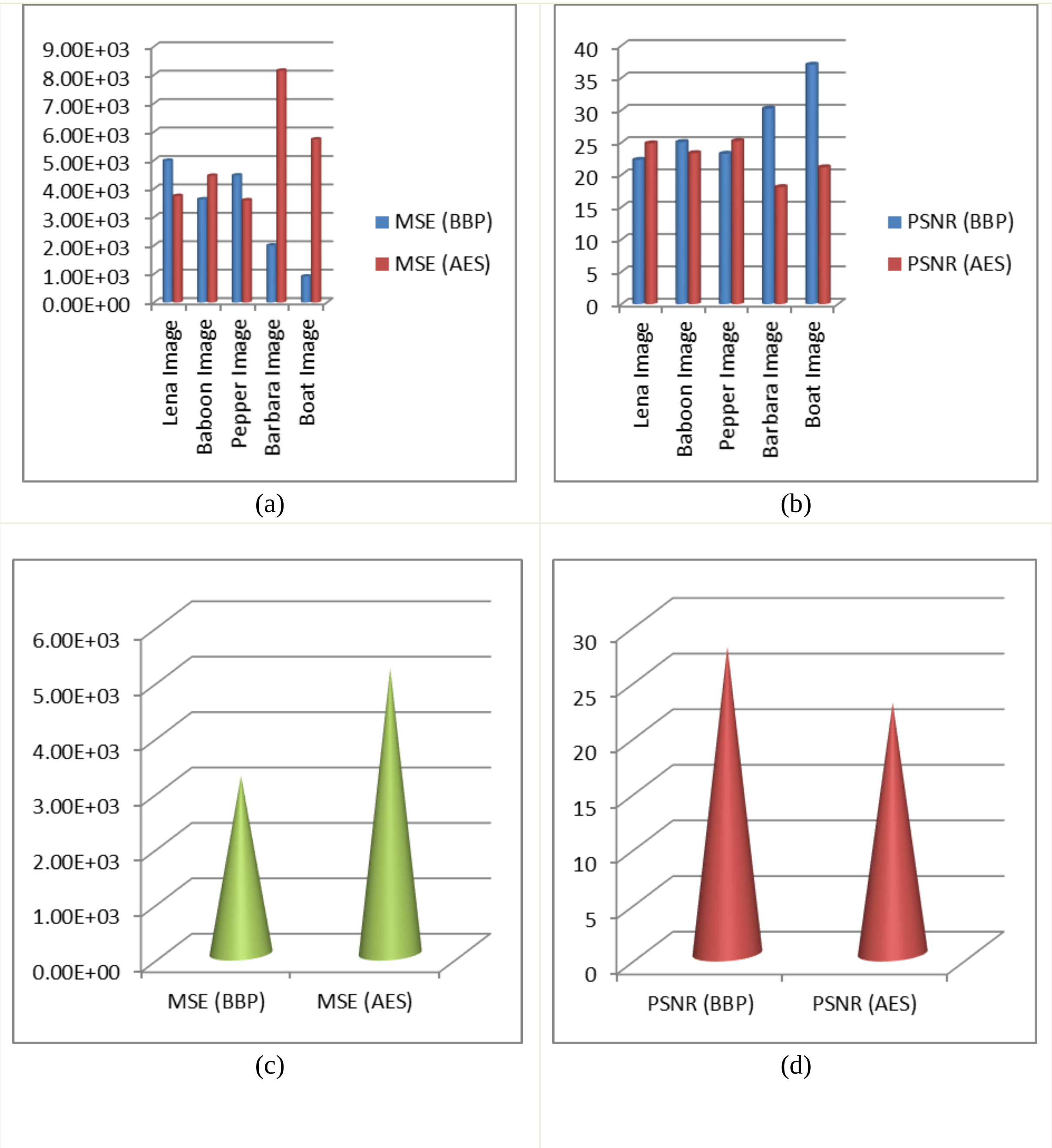
$$\text{Compression ratio} = \frac{\text{Uncompressed image}}{\text{Compressed image}} \quad (3)$$

The measured values are tabulated in Table.1 and Table.2 for both the algorithms and the results comparison is shown in Figure.5 and Figure.6 in graphical format.

S.No	Image Name	Block Based Perceptual (BBP)			Advanced Encryption Standard (AES)		
		MSE	PSNR	CR	MSE	PSNR	CR
1	Lena Image	4.9836e+03	22.3108	4.8621	3.7443e+03	24.8621	10.7789
2	Baboon Image	3.6281e+03	25.0679	3.7488	4.4567e+03	23.3493	10.7789
3	Pepper Image	4.4672e+03	23.2609	4.5689	3.5931e+03	25.2201	10.7789
4	Barbara Image	2.005e+03	30.2389	4.0703	8.1532e+03	18.1028	8.7897
5	Boat Image	914.5351	37.0376	4.0927	5.7355e+03	21.1581	9.1429
	Average Values	**3.20e+03**	**27.5832**	4.2686	**5.14e+03**	**22.5385**	10.0539

Table.1 Performance Results of Block Based Perceptual and Advanced Encryption Standard for Standard Test Images

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731



(a) (b)

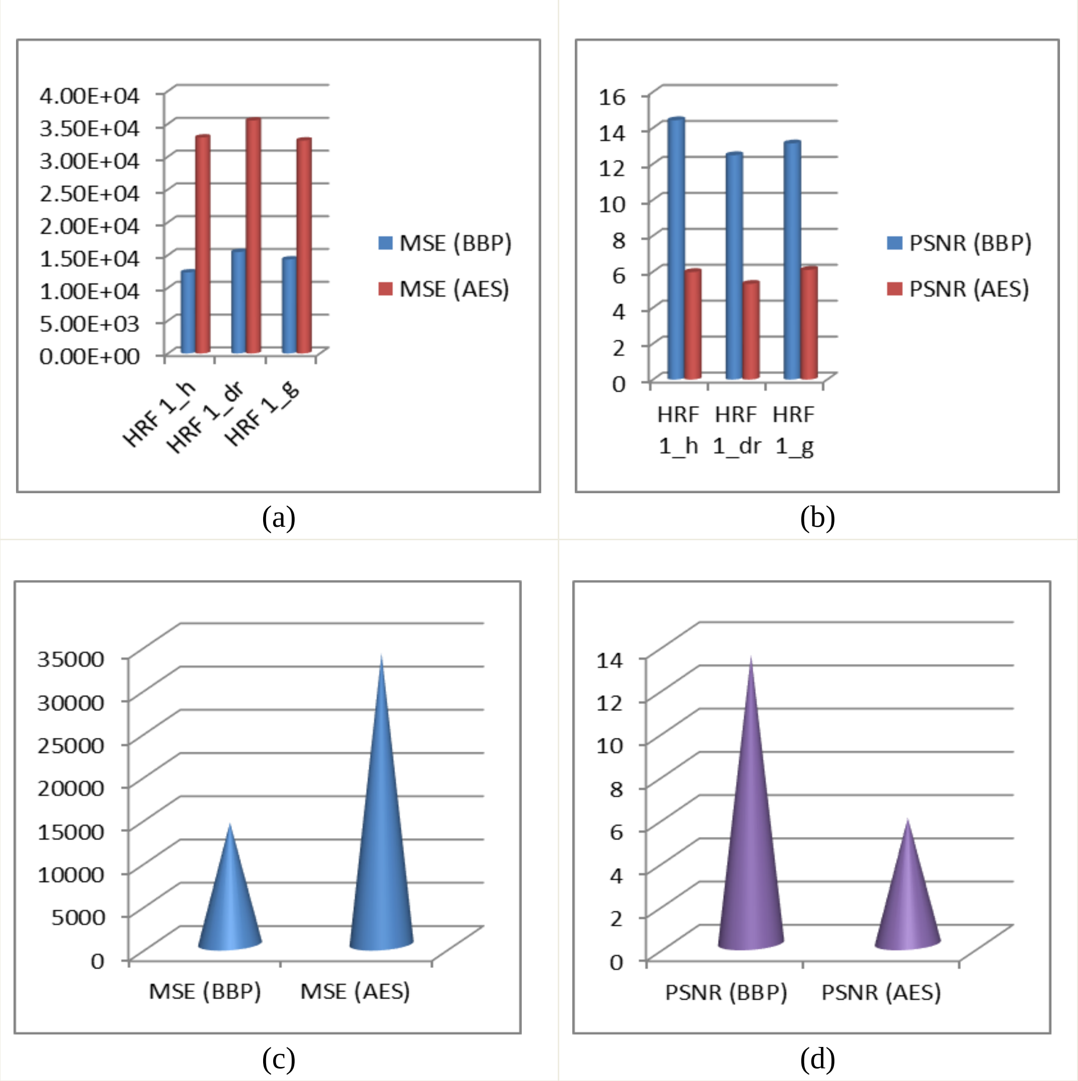
(c) (d)

Figure.5. (a) MSE Comparison Results (b) PSNR Comparison Results (c) MSE Average Value Comparison Results (d) PSNR Average Value Comparison Results for standard test images.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Table.2 Performance Results of Block Based Perceptual and Advanced Encryption Standard for High Resolution Fundus (HRF) Images

S.No	Image Name	Block Based Perceptual (BBP)			Advanced Encryption Standard (AES)		
		MSE	PSNR	CR	MSE	PSNR	CR
1	HRF 1_h (Healthy)	1.2352e+04	14.4268	6.7230	3.2918e+04	5.9809	4.1207
2	HRF 1_dr (Diabetic Retinopathy)	1.5455e+04	12.4804	7.7954	3.5509e+04	5.3229	4.0595
3	HRF 1_g (Glaucoma)	1.4331e+04	13.1358	7.9236	3.2460e+04	6.1027	4.1083
	Average Values	**1.4046e+04**	**13.3477**	7.4807	**3.3629e+04**	**5.8022**	4.0962



(a) (b) (c) (d)

Figure.6. (a) MSE Comparison Results (b) PSNR Comparison Results (c) MSE Average Value Comparison Results (d) PSNR Average Value Comparison Results for HRF Images

Table.3 Comparison of Performance Results of Block Based Perceptual and Advanced Encryption Standard for Standard Color Test Image and High Resolution Fundus (HRF) Images

S.No	Image Name	BBP Method		AES Method		%	%
		MSE	PSNR	MSE	PSNR	MSE	PSNR
1	Standard Color Test Images	3200	27.5832	5140	22.5385	37.74 less	18.29 rise
2	HRF Images	14046	13.3477	33629	5.8022	58.23 less	56.53 rise

From the Table.3 it was clarified that for the standard color test images the BBP method has 37.74% decrease in the MSE value compared to the AES method and also inferred that BBP method shows 18.29% increase in the PSNR values compared to the AES method which indicate higher quality of encrypted image obtained in the BBP method. Similarly for the HRF images the BBP method has 58.23% decrease in the MSE value compared to the AES method and also inferred that BBP method shows 56.53% increase in the PSNR values compared to the AES method

From the above results it was also observed that, the BBP method works well for the medical images compared to the standard color test images as it gives better increase in PSNT and lower in MSE values. Considering the results yielded, we conclude that the block-based perceptual encryption is much better that the AES algorithm and can be implemented for real time medical image data transformation.

4. Conclusion

The implementation of block-based perceptual encryption and AES algorithm has been studied with respect to the standard color test images and HRF Images. Further analyzed the performance parameters such as MSE, PSNR and CR. The two algorithms show acceptable levels of perceptibility and image quality also remains good after decryption. As can be observed from the results for both the standard test images and medical HRF Images, the block based perceptual encryption shows better PSNR values as compared to AES algorithm. The higher PSNR values ensure that the Block based perceptual method means the image quality of the encrypted image is better as compared to the AES algorithm. The BBPE method attains PSNR of 27.58db , MSE of 3.20e+03 and CR of 4.27 for standard test images and 13.35db, 1.4046e+04 and 7.28 respectively for medical HRF images. The BBPE algorithm can be used in Telemedicine and medical transcription.

References

[1]. Afseen Bano, Prateek Sing 2019 Image encryption using block based transformation algorithm. The Pharma Innovation Journal 8(3): 11-18.

[2]. Kundankumar Rameshwar, Vishal Prakash, Amit Kumar Mishra 2014 Text and Image Encryption Decryption Using Advanced Encryption Standard. International Journal of Engineering Trends & Technology in Computer Science 3(3): 118-126.

[3]. Roshni Padate, Aamna Patel 2014 Encryption and Decryption of Text Using AES Algorithm. International Journal of Emerging Technology and Advanced Engineering 4(5): 883-886.

[4]. Ashwini R. Tonde, Akshay P. Dhande 2014 Review Paper on FPGA Based Implementation Of Advanced Encryption Standard (AES) Algorithm. International Journal of Advanced Research in Computer and Communication Engineering 3(1): 4878-4880.

[5]. Karthigaikumar P, Soumiya Rasheed 2011 Simulation of Image Encryption using AES Algorithm. IJCA Special Issue on Computational Science - New Dimensions & Perspectives : 166-172.

[6]. Reza Moradi Rad, Abdolrahman Attar, Reza Ebrahimi Atani 2013 A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR. International Journal of Signal Processing, Image Processing and Pattern Recognition 6(5) : 275-290.

[7]. Divya V.V. Sudha S.K, Resmy V.R. 2012 Simple and Secure Image Encryption. International Journal of Computer Science Issues 9(6) : 286-289.

[8]. Radhadevi P, Kalpana P 2012 Secure Image Encryption Using AES. International Journal of Research in Engineering and Technology 1(2): 115-117.

[9]. Jolly Shah, Vikas Saxena 2011 Performance Study on Image Encryption Schemes. International Journal of Computer Science Issues 8(4) : 349-355.

[10]. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma 2010 Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm). International Journal

of Computer Technology and Electronics Engineering 1(3) : 07-13.

[11]. Attila Budai, Joachim Hornegger, Georg Michelson 2009 Multiscale Approach for Blood Vessel Segmentation on Retinal Fundus Images : In Invest Ophthalmol Vis Sci.50 : 325

[12]. Lakshmi R. Nair , Kamalraj Subramaniam , G. K. D. PrasannaVenkatesan,· P. S. Baskar , T. Jayasankar, “Essentiality for bridging the gap between low and semantic level features in image retrieval systems: an overview”. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02139-z

[13]. Kavitha R.J., Avudaiyappan T., Jayasankar T., Selvi J.A.V. (2021) Industrial Internet of Things (IIoT) with Cloud Teleophthalmology-Based Age-Related Macular Degeneration (AMD) Disease Prediction Model. In: Gupta D., Hugo C. de Albuquerque V., Khanna A., Mehta P.L. (eds) Smart Sensors for Industrial Internet of Things. Internet of Things (Technology, Communications and Computing). Springer, Cham.pp.161-172 https://doi.org/10.1007/978-3-030-52624-5_11

[14]. Kenta Kurihara, Sayaka Shiota, Hitoshi Kiya 2015 An Encryption-Then-Compression System for JPEG Standard. IEEE conference Picture Coding Symposium 119-123.

[15]. Shaohui Liu, Anand Paul, Guochao Zhang, Gwanggil Jeon 2015 A game theory-based block image compression method in encryption domain. The Journal of Supercomputing. 71(9) : 3353-72.

[16]. Mohamed Yacin Sikkandar, T. Jayasankar,· K. R. Kavitha, N. B. Prakash, Natteri M. Sudharsan,G. R. Hemalakshmi, “Three Factor Nonnegative Matrix Factorization based HE Stain Unmixing in Histopathological Images," Journal of Ambient Intelligence and Humanized Computing (2020), https://doi.org/10.1007/s12652-020-02265-8

[17]. J. Jayanthi · E. Laxmi Lydia · N. Krishnaraj · T. Jayasankar · R. Lenin Babu · R. Adaline Suji,” An effective deep learning features based integrated framework for iris detection and recognition,” J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02172-y

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731