International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

A Parallel Processing Technique Based on GMO and BCS for Medical Image Encryption

Vineet Kumar Singh, Piyush Kumar Singh, K.N. Rai

Abstract*: Image encryption is a technique that provides security to an image and their data from unauthorized access in which there is the lightweight process (LWP) that can be parallelized resulting in the reduction of computation time. In this paper, parallel lossless image encryption, as well as the decryption technique, is proposed. The method is a parallel implementation of group modulo operation (GMO) based bit circular shift (BCS) of pixel bit-plane values. The backbone of this technique is circular bit rotation based on some modulo group key value. The key value used here is the result of group modulo operation. The binary bit values of pixels of the initial Image are rotated circularly to generate a new binary bit value of pixels encrypted image. The enhancement of this GMO and BCS based encryption are also given here by using the parallel implementation of the algorithm. The given results show the parallel implementation technique has the same level of encryption standard but has a better level of the time standard. As discussed in the result section, this technique can be used for medical image encryption as well as in multimedia applications where the transfer of image data is required over a network.

Keywords*: Parallel Computing, Medical Image Processing, Group Modulo Operation (GMO), Bit Circular Shift (BCS), Image Encryption-Decryption.

I. INTRODUCTION

Digital image processing is the field which supports and is rapidly used in many different areas such as medical image processing, computer-based photography, satellite imaging, pattern recognition, microscopic imaging, remote sensing, network-based transmission, object detection, surveillance, video processing, transformation feature based security, encryption and decryption, image enhancement and restoration, processing of high-dimensional image data, 3D medical imaging application etc. There are some matrix-based operations that contain a large set of information processing, which consumes much more time during processing. A big challenge is to reduce the processing time.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Vineet Kumar Singh*, DST-CIMS, Institute of Science, BHU, Varanasi, ,(Uttar Pradesh) India. Email: vineet.jpgc@gmail.com, vineet.singh3@bhu.ac.in
P. K. Singh, Deptt. of C.S., Central University of South Bihar, Gaya, Bihar , India. Email: piyushkumarsingh87@gmail.com
Kabindra Nath Rai, Dept. of Mathematical Sciences, IIT-BHU, Varanasi,(Uttar Pradesh) India. Email: knrai.apm@itbhu.ac.in

Parallel processing is a technique in which one or more than one task is executed by more than one processors/cores of a computer system simultaneously.

Parallel processing is a better technique to maintain or reduce time during processing with respect to sequential processing. In the similar manner parallel encryption/decryption process are faster fast will have less elapse time than serial encryption or decryption process. By parallel processing, we can increase the work efficiency of the computer system. The work given here is an initiative to utilize the available architectures in our previous work as given in [1] and [2]. This work is implementation of the parallel version of GMO-BCS based encryption on commonly available computers having multiple cores. The work is lossless image encryption which can be implemented on medical images containing important information at large scale [3]. Parallel computing can provides great opportunity to handle medical images having large data by using a single processor with multiple cores [4]. Processing of these types of images that has large information and are big in size, results in wastage of time that can be overcome by parallelization of color components of images.

II. RELATED WORKS

On the basis of Flynn's classification for fast processing computers, computing hardware classified into 4 types i.e. SISD (Single Instruction Single Data), SIMD (Single Instruction Multiple Data), MISD (Multiple Instruction Single Data), MIMD (Multiple Instruction Multiple Data) depicted in Fig.1 [5, 6]. Where, MISD have no practical (commercial use). The parallelism in SISD can be achieved through the pipelining, where as in SIMD and MIMD the parallel processing can be achieved through pipelining as well as through parallel programming. Parallel computing is a technique, in which numerous computations or calculations are performed at the same time. The details about the MIMD/SIMD architectural paradigm are also described in [7]. A review based on the utilization of GPU (Graphics Processing Unit) used to speed up medical imaging technique is presented in [8]. The conclusion of the review [8] is that medical image processing methods can be useful by using data parallelism based on GPU processing. A high-performance GPU especially designed for computer games is most beneficial for medical image processing by using a hybrid CPU-GPU combination. The difference between GPU and CPU and medical image processing based on GPU, described by some researchers are given in [8].

Parallel computing can be completed, either by multi-core computer, distributed computer or workstation computers. A multi-core CPU approach based on MATLAB is briefly described in [9]. Types of common parallelism are task parallelism, data parallelism and pipeline parallelism [10]. Because of the more time complexity of image processing applications, they cannot meet the real-time need by using a single general purpose processor.

The algorithm speed can be increased using by parallel computing.

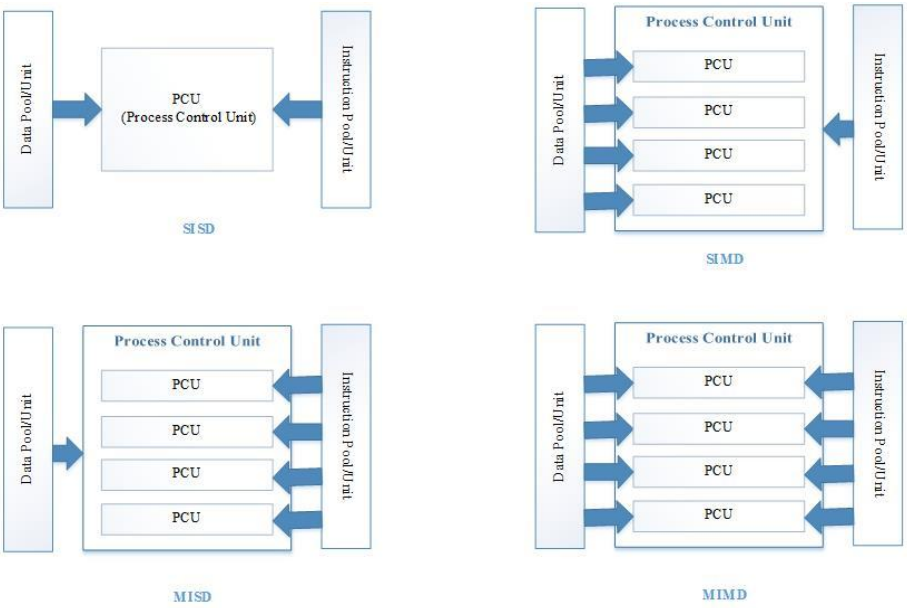

Fig.1 SISD, SIMD, MISD and MIMD

A new parallel image encryption and decryption technique is proposed in [11] by using cloud resources. In this technique, encryption has been done by using FFT, in which two-dimensional matrix are constructed, first one is real and the second one is an imaginary portion of the image. For distributed memory pattern, a low-level data and task parallel image processing is given in [12]. It describes a joint effect of parallelization of i-image processing operators performed by data decomposition using algorithmic framework, and ii-parallelization by task decomposition for image processing applications. For better speed-up seize the opportunity to spring up the task and data parallelism, i.e. a natural process [12]. A parallel chaos-based encryption algorithm using multi-core processors are introduced, in that the parallel algorithm is designed with a master-slave technique. In this technique, the task is allocated to the slave and controlled by the master process [13].

A parallel library based transparent parallel image processing architecture proposed in [14] for application software to users. In [14], an architecture and parallelization pattern in low-level image processing is also discussed. Finally, an APIPM (Abstract Parallel Image Processing Machine) and APIPM based performance model are discussed. In [15], CUDA (Compute Unified Device Architecture) technique based digital image processing through parallel computing is described, in which the evaluation before the calculation is done without parallel computing, with CPU and GPU. In [16], a brief discussion is given about the applications of HPC (High-Performance Computing), which is image processing and computer vision and their barriers i.e. interfaces, cost, size and so on. In continuation of HPC, a historical description of ALVINN (Autonomous Land Vehicle in a Neural Network) and current research during 1994 are also discussed in [16].

A technique for medical diagnosis i.e. high-speed ultrasound volumetric imaging system is developed in [17], which discussed about the design, application and evaluation of parallel processing. A novel image encryption technique for image transfer securely through internet and image compression encryption scheme for multimedia application based on the internet is proposed in [18], in that DWT (Discrete Wavelet Transform) and DES (Data Encryption Standard) algorithm are used for source coding and image encryption. A multi-core architecture and their applications in medical imaging by using parallel computing of sequential image processing algorithm are discussed [19], in which the load of work in divided and distributed in between processors according to requirement. After then, parallel segmentation is applied on images by region growing; global thresholding and then complex noise reduction algorithm are applied.

A parallel motion estimation algorithm proposed and executed by using OpenCL (Open Computing Language) in heterogeneous computer and optimization strategy witch distribute workload in the heterogeneous computer system [20]. Some other discussion about parallel computing and their applications in the area of medical imaging, image registration, reconstruction, image de-noising including 4D, motion estimation and high-order data visualization are given in [21], that covers various imaging technologies such as MRI, CT Scan, X-ray imaging, Optical Tomography, USG imaging, PET etc. In 1975, C. D. Stamopoulos discussed about typical processors with circuit technology, that allow constructing large size arrays that are interconnected parallel logic elements, that results in real-time parallel machines [22]. The application of this processor is discussed in [22], these are also applicable in image processing, artificial intelligence and pattern recognition.

In [23], a framework regarding architectural and programming point of view for parallel computing are described. Computing ability of microprocessor is very low for certain applications. To increase the capability of microprocessor programming and architectural aspects is important and used MIMD or SIMD structure parallelism. Image and video are practical domains, which are very important in parallel computation techniques [23]. An analytical analysis related to distributed and parallel image processing is given in [24],

which describe the parallelism, possibilities, and applicability in image processing applications. Parallelism can also be applied in image processing by three ways i.e. (i) Data parallelism, (ii) Task parallelism and (iii) Pipeline parallelism [24]. The operation of image processing is categorized in three levels i.e. low level, an intermediate level and a high-level image processing [24, 25]. A review related to parallel image processing techniques, their benefits and limitations, purpose, available parallel architecture, tools and techniques that are applying in parallel processing for images, problems related to implementation and role of parallel image processing in medical imaging area are described in [25]. Some description is also given about cores of GPU and CPU, performance and importance of GPU and differences in between the both [25].

A fast color image compression technique through parallel processing based on Wavelet transform is developed in [26], which calculate the convolution-based Wavelet transform for RGB channels of a color image. The work is based on task parallelism, which is calculated and compared with nonparallel image compression technique in the same environment and same computer system [26]. Binary-swap compositing by using parallel volume rendering is discussed in [27], in which the algorithm is performed on assigned data and computation is performed to each individual node of the processor. The binary swap composition proposed in [27] for large data set, is suitable for massively parallel processing.

Image encryption algorithm using variable circular shift proposed in [28], in which a key and an image are used as an initial image. Further more, key Dependant no of bytes group into a block of different sizes. Shifting are done by circular bit rotation where the vacant bit position filled by shifted bits [28].

The proposed methodology is an extension of my own works [1], [2] in which an image encryption algorithm was developed. The circular shift is applied on binary bits of image pixels based on Group modulo properties [1]. In this paper, a parallel processing technique applying on encryption algorithm as discuses in [1], which works sequentially for all channels of color medical images. In the earlier (sequential) technique, the processor executes the complex task or calculation one-by-one at a time which redundant much time. In this paper, the parallel technique is applied to the color image to assign all the channels to the number of corresponding workers of processors at a time. The result is compared with the non-parallel technique at the same system configuration and the same environment. The main objective of the proposed work is to show the comparison of time consumption in both techniques with the security of information related to medical imagery data.

III. IMPLEMENTATION

In this paper, we proposed a lossless parallel encryption technique in which numerous computations or calculation are performed at the same time by a circular shifting of binary values that is 8-bit according to the group modulo operation that holds the property of a group. This work is extension of our previous work as given in [1] using the parallel technique. The paper contains a parallel approach applying at the fourth step as in the existing algorithm to have done the encryption process of a color medical image. The algorithm, encryption process at the bit level, the algebraic structure satisfy the property of Group (i.e. Closure, Associative, Existence of Identity and Existence of Inverse property) and it's modulo property is already discussed in [1].

A. Algorithm for Encryption Process

To encrypt a color retinal image, we apply the parallel technique based on GMO and circular shift at bit level for all three channels to create an encrypted matrix corresponding them at the same time as shown in Fig. 2. The algorithm is depicted in Algorithm I, in which the initial shifting of bits according to key=i for the red component, key=i+j for green channel and key=i+j+k are done parallel, that plays a key role in the encryption process. Initial shifting is always less than 8 means d<8, that holds the property of Group as discussed in [1]. In this way, we find the final encrypted color medical image after converge all channel matrix (encrypted RGB) through a parallel approach. The step by step process of algorithm for the encryption procedure is shown in Algorithm-I and the graphical representation of the parallel encryption process is depicted in Fig. 2.

Algorithm-I: Encryption Algorithm

Parallel Encryption Algorithm:

Step 1: Start.
Step 2: Read the color retinal image.
Step 3: Extract Red, Green, and Blue channels of read image.
Step 4: Calculated the row and column of all channel using parallel technique.
Step 5: Apply parallel processing technique to find out bit representation of all intensity values in all channel of read image.
Step 6: Key based group modulo operation apply to generate circular shift at bit level using parallel approach with initial shifting key=i<8 for Red, key=i+j<8 for green and key=i+j+k<8 for blue channel and key incremented by 1 for every next row.
Step 7: Encrypted matrix channel R, G and B generated.
Step 8: Combined all encrypted channels (RGB) channels.
Step 9: Find the encrypted retinal image.
Step 10: End

B. Algorithm for Decryption Process

The algorithm for decryption process is shown in Algorithm-II. It is as similar to the steps that follow in the encryption process, where the initial image is the parallel processed encrypted image (cipher image) to find the original image (plain image). The step by step procedure of algorithm for the decryption process is shown in Algorithm-II.

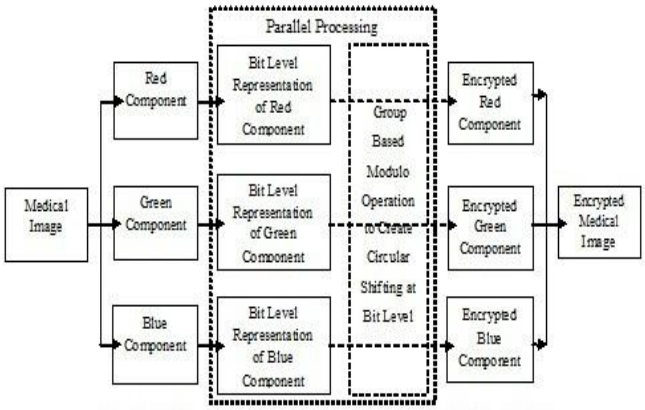

Fig. 2: Parallel Encryption Process Flow

The main difference is that, replacement of key=i by key=8-i for red channel, key=i+j by key=8-(i+j) for second channel i.e. green and key=i+j+k by key=8-(i+j+k) for blue channel. The starting shifting is also less than 8 means key<8 as described in the encryption process. The graphical representation of parallel decryption process shows in Fig. 3.

Algorithm-II: Decryption Algorithm

Parallel Decryption Algorithm:

Step 1: Start.
Step 2: Read cipher color retinal image.
Step 3: Extract Red, Green, and Blue channels of read image.
Step 4: Calculated the row and column of all channel using parallel technique.
Step 5: Apply parallel processing technique to find out bit representation of all intensity values in all channel of cipher image
Step 6: Key based modulo group operation apply to generate circular shift at bit level using parallel approach with initial shifting key=(8-i)<8 for red, key=(8-(i+j))<8 for green and key=(8-(i+j+k))<8 for blue channel and key incremented by 1 for every next row.
Step 7: Generate decrypted matrix of channel matrix R, G and B.
Step 8: Combine all decrypted channels (RGB) channels.
Step 9: Find the decrypted retinal color image.
Step 10: End

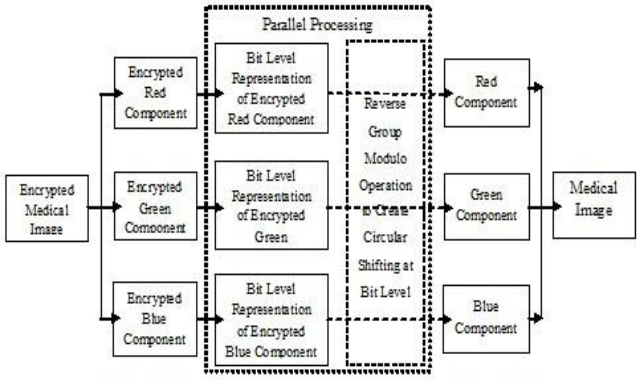

Fig. 3: Parallel Decryption Process Flow

C. PSNR & MSE

The PSNR and MSE values for all channels of all images after encryption in the non-parallel technique are depicted in Table-V. In the parallel technique, the PSNR and MSE values for all channels of all images after encryption are depicted in Table-VII. The PSNR and MSE values of all channels for all images after decryption in non-parallel technique are depicted in Table-VI while in parallel technique, the PSNR and MSE values of all channels for all images after decryption are depicted in Table-VIII. There is no difference in between PSNR and MSE results after encryption as well as decryption results in both non-parallel and parallel techniques means the error is nothing that proves that the proposed technique is totally lossless and parallel approach is better in comparison to non-parallel. The Peak Signal-to-Noise Ratio (PSNR) is calculated as [25]:

$$PSNR=10\ log_{10}\left(\frac{MPV^2}{MSE}\right) \quad (1)$$

Where, M=maximum P=pixel and V=value. The decibel (dB) unit is used for PSNR.

The Mean Square Error (MSE) calculated between plain image and cipher image before decryption. After decryption, MSE calculated between plain image and decrypted image as per equation (2) [25]:

$$MSE=\frac{1}{rc}\sum_{i=0}^{r}\sum_{j=0}^{c}(X[i,j]-Y[i,j])^2 \quad (2)$$

Where r= row, c=column values, X contains the original image and Y is the resultant (after encryption) image stored in the form of matrices.

IV. EXPERIMENTAL RESULTS

The experimental results section contains two sections. First section contains the encryption results and the second section shows the decryption results. The experimental result also shows the comparative study in between non-parallel technique and parallel techniques.

A. Encryption Results

The algorithm for decryption process is shown in Algorithm 2. The encryption results for img0001 to img0005 are shown in Fig.4 to Fig.8 simultaneously and the times consuming in both techniques are depicted in Table-I and Table-II after the experiment did. To reduce time complexity, parallel computing can be used where numerous computations or calculations performed at the same time. In this paper, we proposed a parallel technique for bit circular shift based on GMO, applying on binary values of an image pixel. In this paper, the algorithm was applied to five color retinal images of size between 41.1 KB to 49.3 KB for performing the experiment. The dimensions are same for all images i.e. 512x512. Firstly, we did the experiment for non-parallel technique and then execute the parallel technique for img0001 and the same for img0002, img0003, img0004 and img0005. We execute the program ten times in ideal condition for non-parallel technique and also ten times for parallel technique. In parallel processing, we assigned all three RGB channels of medical image separately to the corresponding workers (CPU cores) of the processors at the same time. After comparison, we find that the performance of the parallel technique is much better than the non-parallel technique for all images. The average times after encryption in the non-parallel technique for all images that we have taken after processing is shown in Table-I.

Whereas the parallel encryption average time for img0001 to img0005 depicted in Table-II.

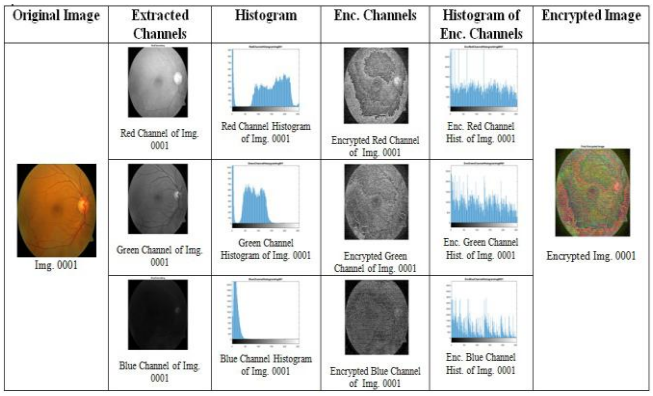

Fig.4. Encryption Result for img0001

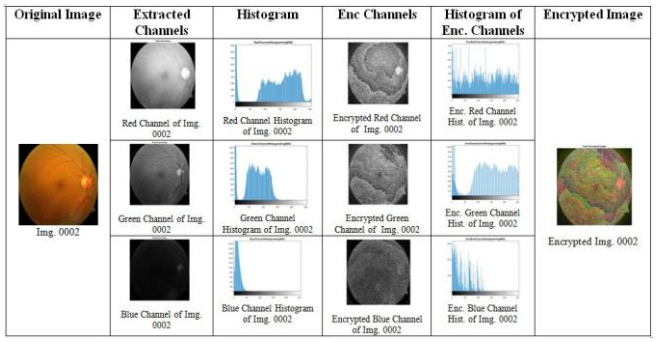

Fig.5. Encryption Result for img0002

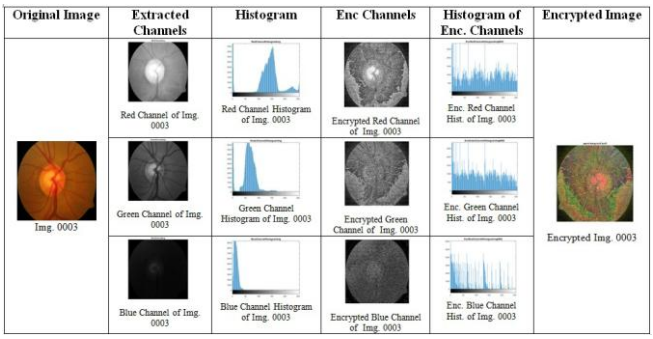

Fig.6. Encryption Result for img0003

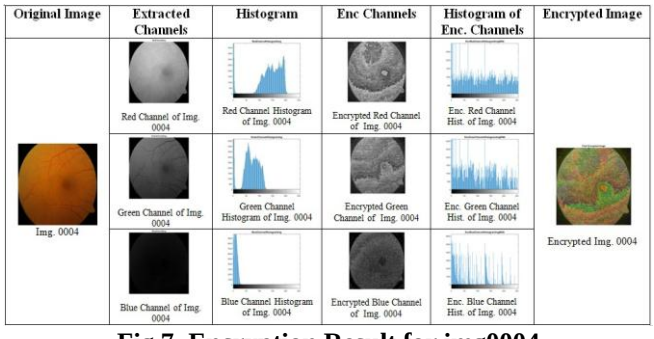

Fig.7. Encryption Result for img0004

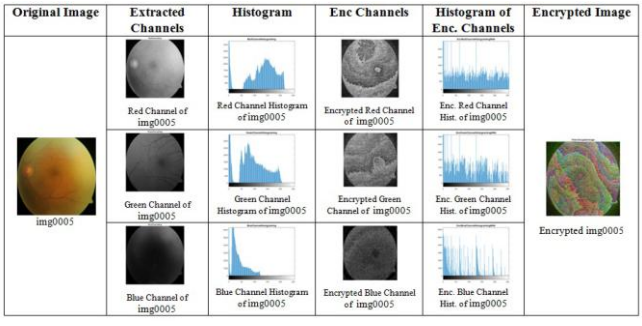

Fig.8. Encryption Result for img0005

B. Decryption Results

The decryption results for img0001 to img0005 are shown in Fig.9 to Fig.13 simultaneously. After the decryption process is done, the average time is shown in Table-III for non-parallel technique while the average decryption time for parallel technique is depicted in Table-IV.

According to the average time comparison after decryption in both, parallel technique is much better and preferable in comparison to the non-parallel decryption process. For img0002, parallel decryption time is better but near to the non-parallel decryption technique as we seen earlier in encryption process. The parallel decryption process time for img0001 and img0005 is much better in comparison to non-parallel decryption technique that is depicted in Table-IV. It is seen very easily that the decryption time is less in parallel technique. It is similar as in the case of the encryption process. This means that the encryption and decryption both techniques which have multiprocessing approach, gives much better results. The decryption process time in non-parallel technique is much higher than the decryption process in parallel technique. However the results are analogous in the parallel technique that is the less time taken in the decryption process.

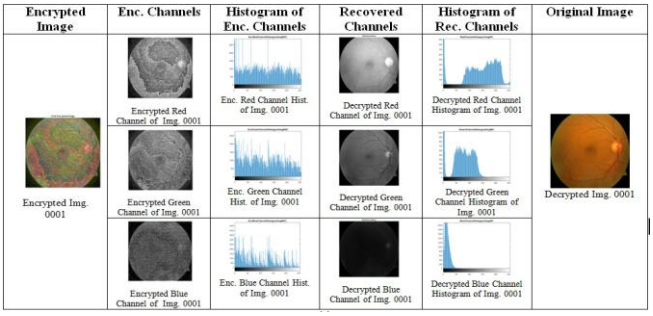

Fig.9. Decryption Result for img0001

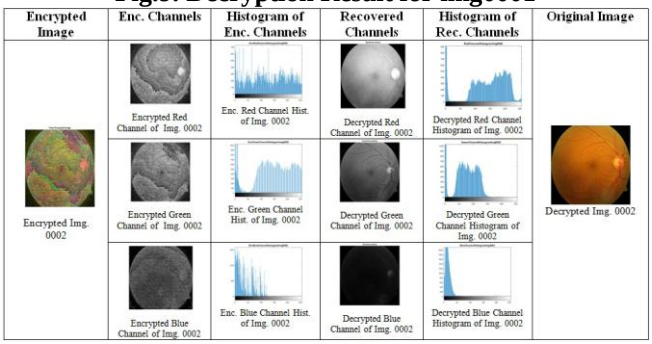

Fig.10. Decryption Result for img0002

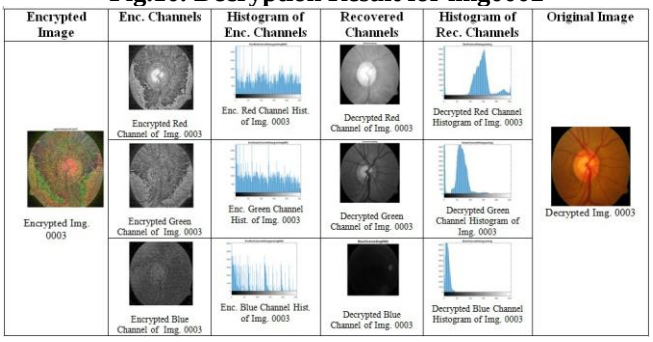

Fig.11. Decryption Result for img0003

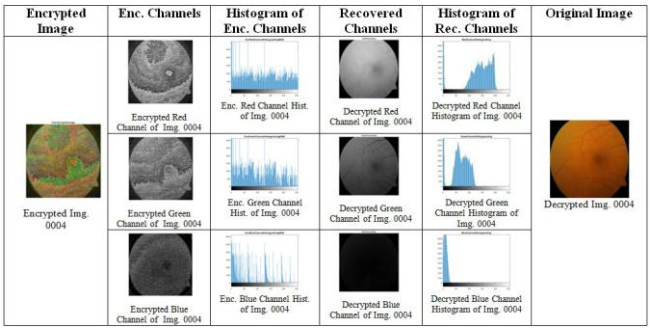

Fig.12. Decryption Result for img0004

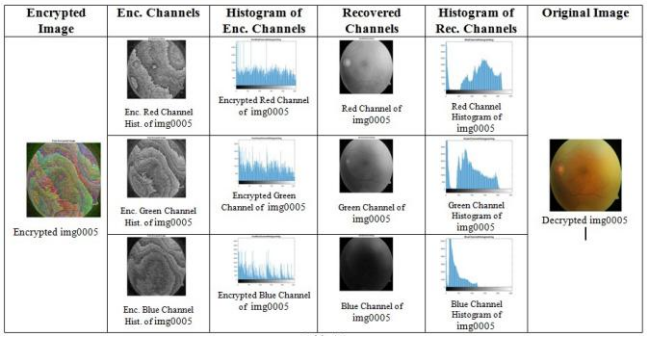

Fig.13. Decryption Result for img0005

The tabular results of the decryption and the encryption process are also mention in terms of the MSE and PSNR. The values of the MSE and PSNR are shown in the same table for comparison. The Level of the encryption and the level of decryption both are comparable in term of the MSE and PSNR. The values are exactly same as shown in the Table 5 and 7 below.

The graphical representation is also shown in the line graph mentioned below Fig. 14 and Fig. 15. These graphs are representation the comparative analyses in the pictorial form. The pictorial forms are quite helpful in the case of understanding and analysis.

V. RESULT DISCUSSION

The experimental result shows the time comparison between parallel and nonparallel techniques for both encryption and decryption processes. The processing time consumed in non-parallel technique for img0001-img0005. The experiment is repeated is 10 times on each image and the result are depicted in Table 1. Similarly the time consumed the parallel technique for img0001-img0005 is depicted in Table 2. The Time measured in seconds up to six decimal places. As per results depict in Table 1, Table 2, Fig. 14 and Fig. 15, the parallel encryption technique is much better in comparison to sequential encryption techniques. On the basis of results it may preferable for all medical image encryption. For img0002 parallel encryption, time is better but near to non-parallel encryption technique. In comparison to both techniques, the average time in the parallel encryption technique is much better than the non-parallel technique for all images.

After seeing the results, it is clear that a time taken in case of the parallel group modulo based circular shift is less than the non-parallel group modulo based circular shift algorithm. The time taken in case of the parallel technique should be one third to the time taken in non-parallel technique as the algorithm parallelizes the three color channels. But it is not exactly the one third due to communication delays as it is only theoretically possible in case of ideal situation [29]. The histogram shown in the Fig. 4 to Fig. 13 depicts the variation of frequencies in case of the encrypted image and the decrypted image. The histogram of the encrypted images shows a nice characteristic that the histogram equalizes, showing a nice encryption technique. The equalization of histogram shows the pixels having similar intensity values are almost equal in numbers. The decryption process shows the histogram of all the channels of the image is exactly same to the original color channels of the images. The peak-signal-to-noise ratio (PSNR) and mean square error (MSE) is depicted in Table 5 and Table 7 showing the quantitative description of the encryption technique. The Table 6 and Table 8 represents that the encryption technique is purely lossless as the MSE between each components of the original images and decrypted images is found to be zero. Similarly the PSNR between original and encrypted image is infinite for each of its component.

The graph shown in Fig. 14 and Fig. 15 shows the superiority of parallel technique with respect to non-parallel technique for both encryption and decryption process. The graph is plotted taking average of the ten iterations for each image.

VI. EXPERIMENTAL PLATFORM

The system configuration for doing the experiment, we used Machine DELL OPTIPLEX 980 Intel(R) Core(TM) i5 CPU 650@ 3.20 (3.19) GHz Processor with 4 GB RAM (3.43 GB usable), System type 32-bit Operating System (Windows 7 Professional) environment (Processor Intel(R) Core(TM) i5 CPU 650 @ 3.20GHz,3193 Mhz, 2 Core(s),4 Logical Processor(s)).

Table- I: Encryption Times in Non-Parallel Technique

No. of Time	Img0001	Img0002	Img0003	Img0004	Img0005
1	432.26119	440.633317	422.499409	391.495622	456.704157
2	435.588484	437.086596	387.424791	385.469958	449.955327
3	437.169474	442.808316	400.350373	394.633141	453.846838
4	434.818727	441.140855	393.910193	399.619884	454.001100
5	439.876829	441.883693	399.115537	399.445493	452.711060
6	439.399009	445.536581	400.745877	395.239607	451.017992

7	451.751923	444.763678	399.430601	399.065756	458.207157
8	453.617646	441.821185	400.707077	398.125504	450.324122
9	453.458047	443.620009	404.541161	398.843288	451.514260
10	457.877107	442.575582	400.731140	404.534724	477.315247
Average Encryption Time	**443.581844**	**442.186981**	**400.945616**	**396.647298**	**455.559726**

Table- II: Encryption Times in Parallel Technique

No. of Time	Img0001	Img0002	Img0003	Img0004	Img0005
1	418.333375	416.908007	424.440942	391.526455	433.479063
2	409.532768	412.013521	382.233773	383.060329	433.081853
3	403.039989	420.886681	386.234091	374.519922	425.146856
4	408.368088	426.163082	377.069167	377.939085	415.019919
5	406.779217	420.867847	374.177307	373.361877	424.746245
6	402.429056	421.702851	380.28025	377.472778	425.567881
7	405.265063	420.690331	379.791034	373.336554	418.606718
8	405.730966	420.281861	373.43203	380.499541	428.067111
9	403.72989	420.946167	381.36431	372.486871	423.620071
10	405.166351	416.371906	398.689056	383.566988	423.669486
Average Encryption Time	**406.837476**	**419.683225**	**385.771196**	**378.777040**	**425.100520**

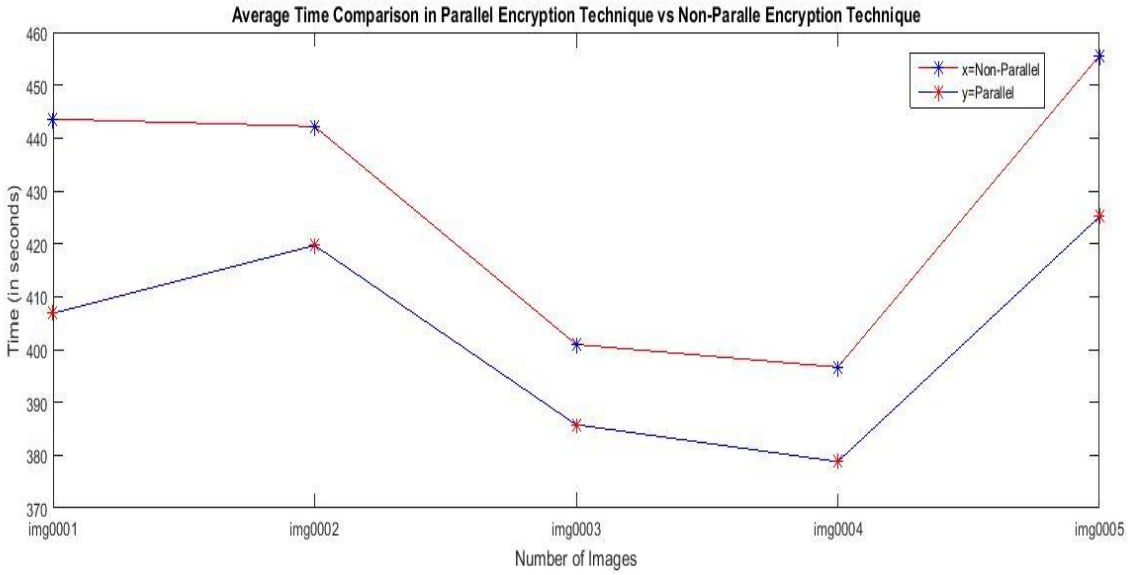

Fig. 14. Average Time comparison of Encryption Process in between Parallel and Non-Parallel Technique

Table- III: Decryption Times in Non-Parallel Technique

No. of Time	Img0001	Img0002	Img0003	Img0004	Img0005
1	435.610083	439.294608	401.28293	405.956367	457.807232
2	439.183878	449.946128	400.884148	404.910612	451.075565
3	433.52191	442.462853	405.229497	396.089422	451.979275
4	433.982354	444.337006	398.933666	396.374459	453.029287
5	433.639433	440.603213	397.547085	398.381413	452.595314
6	434.299867	444.168364	398.873927	401.382846	452.106210
7	454.708972	442.374087	397.909738	406.349455	456.333350
8	447.587817	445.899993	398.257502	400.571038	458.869637
9	450.684329	446.080234	398.892261	405.108915	451.775231
10	453.972021	443.360046	395.953604	424.631561	481.869856
Average Decryption Time	**441.719066**	**443.852653**	**399.376436**	**403.975609**	**456.744096**

Table- IV: Decryption Times in Parallel Technique

No. of Time	Img0001	Img0002	Img0003	Img0004	Img0005
1	409.527548	412.616998	386.292723	382.004010	425.345225
2	405.273815	416.373047	385.730978	378.680988	422.830488
3	404.733095	416.528865	375.922192	375.385010	421.303845
4	406.067943	417.968269	383.309224	379.185472	416.230969
5	400.941191	418.610678	396.247751	381.893454	421.202940
6	397.533095	418.926349	387.930912	380.475235	425.869846
7	406.108072	419.987506	380.450392	379.330165	421.179556
8	405.50584	418.69431	376.420031	381.938427	434.761617
9	400.982171	417.62067	379.989000	382.315407	424.815856
10	403.208138	413.367475	378.278724	382.278872	422.728716
Average Decryption Time	**403.988091**	**417.069417**	**383.057193**	**380.348704**	**423.626906**

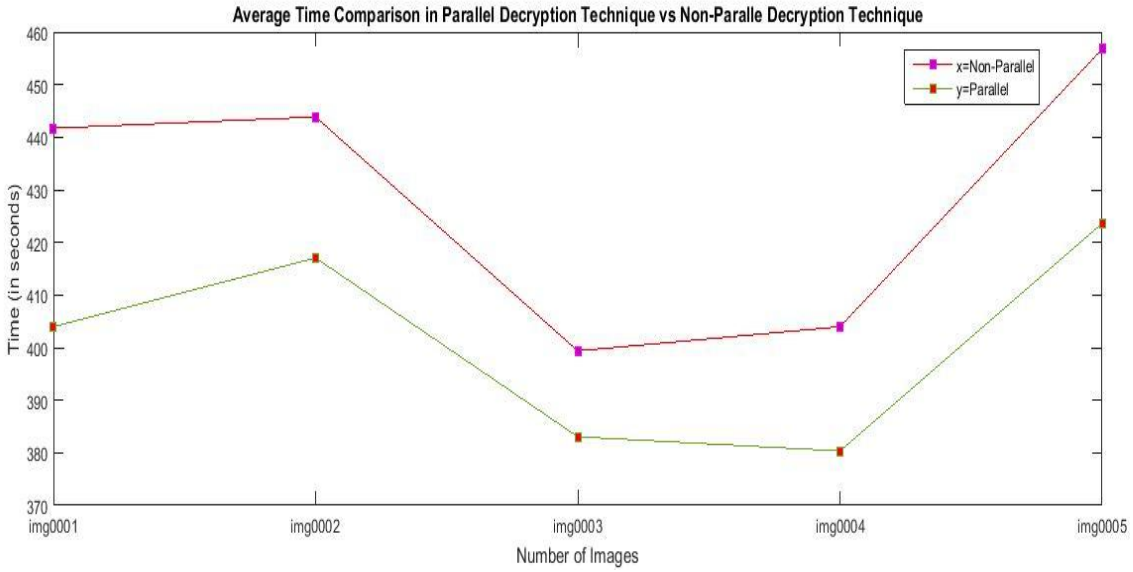

Fig.15. Average Time comparison of Decryption Process in between Parallel and Non-Parallel Technique

Table- V: After Encryption PSNR & MSE in Non-Parallel Technique

PSNR & MSE after Encryption in Non-Parallel Technique										
	Img0001		Img0002		Img0003		Img0004		Img0005	
Channels	PSNR Value	MSE Value	PSNR Value	MSE Value	PSNR Value	MSE Value	PSNR Value	MSE Value	PSNR Value	MSE Value
R	33.8114	108.99	33.7910	109.51	33.8895	107.05	33.8876	107.1	103.51	34.04
G	36.5731	57.71	36.6511	56.68	37.0720	51.45	37.2355	49.54	75.13	35.43
B	42.2138	15.75	43.4282	11.9	43.6018	11.44	45.9429	6.67	29.62	39.47

Table- VI: After Encryption PSNR & MSE in Non-Parallel Technique

PSNR & MSE after Decryption in Non-Parallel Technique										
	Img0001		Img0002		Img0003		Img0004		Img0005	
Channels	PSNR Value	MSE Value	PSNR Value	MSE Value	PSNR Value	MSE Value	PSNR Value	MSE Value	PSNR Value	MSE Value
R	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00
G	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00
B	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00

Table- VII: After Encryption PSNR & MSE in Parallel Technique

PSNR & MSE after Encryption in Parallel Technique										
	Img0001		Img0002		Img0003		Img0004		Img0005	
Channels	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Red	33.8114	108.99	33.7910	109.51	33.8895	107.05	33.8876	107.1	103.51	34.04
Green	36.5731	57.71	36.6511	56.68	37.0720	51.45	37.2355	49.54	75.13	35.43
Blue	42.2138	15.75	43.4282	11.9	43.6018	11.44	45.9429	6.67	29.62	39.47

Table- VIII: After Encryption PSNR & MSE in Parallel Technique

PSNR & MSE after Decryption in Parallel Technique										
	Img0001		Img0002		Img0003		Img0004		Img0005	
Channels	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Red	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00
Green	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00
Blue	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00	Inf dB	0.00

VII. CONCLUSION

In this paper, we proposed a parallel computational technique to reduce the time and furthermore improve the proficiency of algorithms proposed in [1] for medical image encryption technique, based on GMO and BCS. In this experiment, we assign the extracted RGB channels of the original color medical image to corresponding workers (CPU cores) for computation and encryption simultaneously. After the experiment did for all images like img0002, img0003, and img0004 except than img0001, we get the time takes to run parallel algorithm is much better in comparison to the non-parallel technique. It means the parallel technique is highly preferable for medical image encryption rather than non-parallel technique.

Finally, the paper concluded that the parallel technique gives better performance and may be suitable for providing security to medical images in future without any extra hardware effort. In the future, this parallel technique may be used in app-based encryption and decryption for secure medical images transmission. The key points of the conclusion are given below:

1) The algorithm given here is the parallel version of GMO-BCS algorithm as given in [1].
2) The algorithm is exploiting the parallel technique mentioned in [1] on image encryption which can be applied to DICOM (Digital Imaging and Communications in Medicine) images.
3) The algorithm is nice combination of advance computational technique (parallel programming) and theory of abstract algebra (group theory).
4) The algorithm given here is fast in terms of GMO-BCS in every samples of the image.
5) The future work related to this algorithm can be hypothesis testing on infinite population of images taking the experimental results here.

ACKNOWLEDGEMENT

A lot of thanks to Ophthalmologist (eye specialist) Dr. Manoj Kumar, Indian Medicine, SSH, BHU who has provided medical images with description for their guidance and directions as required time to time.

REFERENCES

1. Singh, Vineet Kumar, Piyush Kumar Singh, and K. N. Rai. "Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.
2. Singh, Vineet Kumar, A. Singhal, K. N. Rai, Abhishek Kumar, A.N.D. Dwivedi." Randomized Key-based GMO-BCS Image Encryption for Securing Medical Image." IJRTE, Vol. 8, Issue 3, 2018.
3. Hennessy, John L., and David A. Patterson. "Computer architecture: a quantitative approach." Elsevier, 2011.
4. Wu, Minye, et al. "A parallel processing model for big medical image data." Information Technology and Artificial Intelligence Conference (ITAIC), 2014 IEEE 7th Joint International. IEEE, 2014.
5. Hemnani, Monika. "Parallel processing techniques for high performance image processing applications." Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference on. IEEE, 2016.
6. Christensen, Gary E. "MIMD vs. SIMD parallel processing: A case study in 3D medical image registration." Parallel Computing 24.9-10 (1998): 1369-1383.
7. Duncan, Ralph. "A survey of parallel computer architectures." Computer 2 (1990): 5-16.
8. Khor, Hui Liang, Siau-Chuin Liew, and Jasni Mohd Zain. "A review on parallel medical image processing on GPU." 2015 4th International Conference on Software Engineering and Computer Systems (ICSECS). Vol. 17. No. 8. 2015.
9. Gao, Wenjing, et al. "Parallel computing for fringe pattern processing: A multicore CPU approach in MATLABÂ® environment." Optics and Lasers in Engineering 47.11 (2009): 1286-1292.
10. Bouge, Luc. "The data parallel programming model: A semantic perspective." The Data Parallel Programming Model. Springer, Berlin, Heidelberg, 1996. 4-26.
11. Rad, Paul, et al. "A novel image encryption method to reduce decryption execution time in cloud." Systems Conference (SysCon), 2015 9th Annual IEEE International. IEEE, 2015.
12. Nicolescu, Cristina, and Pieter Jonker. "A data and task parallel image processing environment." Parallel Computing28.7-8 (2002): 945-965.
13. Wang, Xizhong, and Deyun Chen. "A parallel encryption algorithm based on piecewise linear chaotic map." Mathematical Problems in Engineering 2013 (2013).
14. Seinstra, Frank J., Dennis Koelma, and Jan-Mark Geusebroek. "A software architecture for user transparent parallel image processing." Parallel computing 28.7-8 (2002): 967-993.

15. Skirnevskiy, I. P., A. V. Pustovit, and Mariya Ovseevna Abdrashitova. "Digital image processing using parallel computing based on CUDA technology." Journal of Physics: Conference Series. Vol. 803. No. 1. IOP Publishing, 2017.
16. Webb, John A. "High performance computing in image processing and computer vision." Pattern Recognition, 1994. Vol. 3-Conference C: Signal Processing, Proceedings of the 12th IAPR International Conference on. IEEE, 1994.
17. Von Ramm, Olaf T., Stephen W. Smith, and Henry G. Pavy. "High-speed ultrasound volumetric imaging system. II. Parallel processing and image display." IEEE transactions on ultrasonics, ferroelectrics, and frequency control 38.2 (1991): 109-115.
18. Dang, Philip P., and Paul M. Chau. "Image encryption for secure internet multimedia applications." Consumer Electronics, 2000. ICCE. 2000 Digest of Technical Papers. International Conference on. IEEE, 2000.
19. Saxena, Sanjay, Neeraj Sharma, and Shiru Sharma. "Image processing tasks using parallel computing in multi core architecture and its applications in medical imaging." International Journal of Advanced Research in Computer and Communication Engineering 2.4 (2013): 1896-1900.
20. Zhang, Jinglin, Jean-Francois Nezan, and Jean-Gabriel Cousin. "Implementation of motion estimation based on heterogeneous parallel computing system with opencl." High performance computing and communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on. IEEE, 2012.
21. Kadah, Yasser M., et al. "Parallel computation in medical imaging applications." International journal of biomedical imaging 2011 (2011).
22. Stamopoulos, Charalambos D. "Parallel image processing." IEEE Transactions on Computers 4 (1975): 424-433.
23. Merigot, Alain, and Alfredo Petrosino. "Parallel processing for image and video processing: Issues and challenges." Parallel Computing 34.12 (2008): 694-699.
24. Prajapati, Harshad B., and Sanjay K. Vij. "Analytical study of parallel and distributed image processing." Image Information Processing (ICIIP), 2011 International Conference on. IEEE, 2011.
25. Saxena, Sanjay, Shiru Sharma, and Neeraj Sharma. "Parallel image processing techniques, benefits and limitations." Research Journal of Applied Sciences, Engineering and Technology 12.2 (2016): 223-238.
26. Singh, Piyush Kumar, Ravi Shankar Singh, and Kabindra Nath Rai. "A Parallel Algorithm for Wavelet Transform-Based Color Image Compression." Journal of Intelligent Systems 27.1 (2018): 81-90.
27. Ma, Kwan-Liu, et al. "Parallel volume rendering using binary-swap compositing." IEEE Computer Graphics and Applications 14.4 (1994): 59-68.
28. Tamimi, Abdelfatah A., and Ayman M. Abdalla. "A Variable Circular-Shift Image-Encryption Algorithm.", IPCV'17
29. Stallings, William. Computer organization and architecture: designing for performance.(6e), Pearson Education India, 2003.

AUTHORS PROFILE

Vineet Kumar Singh, enrolled as a research scholar and pursues their Ph.D. in Computer Application from DST-CIMS (Department of Science and Technology – Centre for Interdisciplinary Mathematical Sciences, Institute of Science, Banaras Hindu University (BHU), Varanasi. He has completed Master of Computer Application in the year 2011 from Indira Gandhi National Open University, Maidan Garhi, New Delhi. Mr. Singh has appointed as an Assistant Professor in Faculty of Computer Application at Jagatpur Post Graduate College, Varanasi (Affiliated to MGKVP, Varanasi) since September 2011. Mr. Singh has published a Lab Manual for UG students, published three papers Scopus, ESCI and IEEE indexed journal. The research area of Mr. Singh is Image Processing, Image Watermarking. Mr. Singh has a live membership of 'The Indian Science Congress Association', Kolkata. He was a former member of IEEE up section up to December 2018.

Dr. Piyush Kumar Singh, is an Assistant Professor in Department of Computer Science, Central University of South Bihar, Gaya, Bihar. Dr. Singh completed B.Sc.(Mathematics, Physics) from Udai Pratap college Campus, Varanasi in 2007 in first division, MCA from RSMT, Udai Pratap College Campus, Varanasi in 2010 in first division and Ph.D. from Banaras Hindu University, Varanasi. Dr. Singh is UGC-NET and GATE qualified. He has awarded UGC Research Fellowship in February, 2015. Dr. Singh has teaching experience from 2010 to 2012 in CHBS (K), Banaras Hindu University, Varanasi. Dr. Singh has numerous publications in different journals. He has also contributed one book chapter entitled "Wavelets with application in Image Compression" published in book entitled "Emerging Technologies in Intelligent Applications for Image and Video Processing" in IGI Global, USA.

Prof. K. N. Rai, is an Emeritus Professor of Indian Institute of Technology (Banaras Hindu University) since July 2019. Prof. Rai was a former Institute Professor of IIT (BHU) from January 2015 to June 2019 and has achieved HAG scale from August 01, 2012 to July 31, 2014. Prof. Rai was a former Professor of IIT (BHU) from October 1994 to July 2012. Including Mathematical Modeling he has an expert of several fields such as Differential Equation, Mathematical Methods, Nonlinear Mathematics, Heat and Mass Transfer, Bio-transport Process, Moving Boundary Problems, Image Processing, etc.. He has 110+ Publications, one published book and three book chapters published. Prof. Rai has 47 years of experience in research and academics. Under the supervision of him, 19+ researchers have completed their Ph.D.. Prof. Rai has achieved an outstanding reviewing award by International Journal of Heat and Mass Transfer, Elsevier. He has achieved a reviewing certificate by International Journal of Heat and Mass Transfer, Elsevier and International Journal of Thermal Science, Elsevier.