# Improving Data Security using Compression Integrated Pixel Interchange Model with Efficient Encryption Technique

## Compression Integrated Pixel Interchange Model

Naga Raju Hari Manikyam[1]
Research Scholar, CSE Department
VelTech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology
Chennai – Tamilnadu. PIN: 600062

Munisamy Shyamala Devi[2]
CSE Department
VelTech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology
Chennai – Tamilnadu. PIN: 600062

***Abstract*—We exist in a digital era in which communication is largely based on the transfer of digital knowledge over data networks. Disclosures are sometimes regarded as a transmitter that transmits a digital file. A system of encoding, efficient and easy yet secure model must be developed for quick and prompt transmission. The file is sent from source to destination where it is difficult to maintain the privacy of knowledge. The encryption of images is vital for securing sensitive information or images from unauthorized readers. By using a technique of selective encryption, the original image pixel values are completely obscured in this way and an intruder cannot retrieve statistical data from its original image. This paper introduces a new methodology for the use of a protective facility for the transmission of digital data over the public network. A highly established field with image compression is allowed for speedy transmission and efficient information storage. During the initial process, the original image is divided into blocks of the same size and sub segmentation is performed for accurate extraction of images within the boundaries. A random matrix is used to swap the pixels of the neighboring sub blocks. Afterwards, each pixel is randomly exchanged for the neighboring blocks with a random matrix, then each block is encrypted with the proposed function and then the encrypted data can be stored in cloud. The proposed method uses Image Segmentation based Compression Model with Pixel Interchange Encryption (ISbCPIE) Model for providing high security to the Image transmitted in the network. Compressor is needed to achieve rapid transmission and efficient storage. The proposed model is compared with the traditional models and the results show that the proposed model security levels are better than the existing models.**

***Keywords*—Image segmentation; image pixel extraction; pixel compression; pixel interchange; image security***

## I. INTRODUCTION

Typically, the quick progress of science and technology has utilized information technology in people's daily lives. During this era of digital data technology, the majority of private data and protected data are exchanged with electronic media [1]. The benefit of using electronic media for the sharing of personal data is that, technological devices convey information or photos in unusual conditions of safety, secrecy and honesty. An encryption framework for secure communication applications has been developed in order to find a response to the problem of security mode. The cryptographic technique is the process used to fix the original message with key to the protection of privacy and integrity of the information [2]. Encryption is a message encoding technique or key information [3]. By using the same key used for encryption, the first message or information will be exposed.

Cryptography can provide a solution, which can only be decrypted when the sender encrypts a message [4]. The aim of this research work is to study the compression and encryption combinations in digital photographs. These are both data compression and encryption processes [5] used to ensure maximum security for photos transferred. Image Segmentation is a process in which a digital image is separated into different subgroups, called Image Objects [6]. This is called Image Object, which can help to minimize the image ambiguity and thereby make the analysis of the image more straightforward. The effect of segmentation affects compression sophisticatedly.

Moore's Law and Storage Law are specifically linked to advances in imaging technology. The techniques needed to store these collected data and to transmit them should be enhanced if the amount of information in the world doubles every 18 months. As a result, the demand for compression techniques is enormous and is considered to be particularly significant in the current knowledge explosives. Image compression solves the problem of lowering the amount of information necessary to deliver the digital image with a decent image quality [7]. Compression of images is currently considered as an activated technology and a natural technique of handling the rising spatial resolution and changing TV broadcast standards of today's image sensor [8].

The proposed ISbCPIE algorithm is used to compress and encrypt images in order to resolve the above disadvantages. A new scalable coding scheme for encrypting images is given. In the encryption process of the proposed scheme, the pixel values are totally obscured. So an intruder cannot get statistical data from his original image. The coded data is then

decomposed into many parts. By combining each part, the bit stream is achieved. Using the cryptographic key on the recipient side, the higher the resolution for the more bit streams the original content is retrieved.

## II. Literature Survey

Aqeel-ur-Rehman et al. [2] researched Quaternion Discrete Cosine Transform (QDCT), which was much more knowledgeable about the difficulty of its conventional equivalents. The adopted QDCT has also been used to create and recognize a method of quantum image compression. The introduced compression model performs a search to determine the most significantly assessed DCT coefficients that has achieved. The added model therefore could simultaneously measure the DCT coefficients by using two predictions. In addition, the examination of the scheme adopted reveals that the scheme was better applied than the other classical models. The feasibility of the proposed solution has therefore been validated over conventional schemes.

A nonlinear, chaotic algorithm based primarily on tangents and power rather than linear functions was proposed by Jallouli et al. [3]. In order to provide multilevel security, S-box on chaotic maps are utilized. Here, with the aid of a logistic map and a 2D map, authors created dynamically 8/8 S-box. The first division in the plain image was 8 block sizes, followed by the blockbased shuffling of the image by a 2D map process in three separate chaotic maps. The shifted image is encrypted using a chaotic 1D logistic map sequence.

A new image encryption method has been introduced by Jiang et al. [6], which first arranges the image pixels based on RGB values and then transfers the intermediate image for encryption. The proposed image encryption algorithm and its security analysis as key space analysis, statistical analysis and differential analysis were defined in detail. The aim of chaotic key-based algorithm CKBA was to increase protection, with a discrete wavelet transformation and modified Key-base algorithm. Cryptanalysis has been carried out to examine the increased safety of the proposed algorithm. A permutation technique based on the three independent Diophantine equations system resolution has been implemented. An efficient chaotic block cipher with a chaotic logistic map has been suggested from this permutation algorithm. Luo et al. [7] proposed a random bit sequence generator algorithm, which was based on chaotical maps for image encryption. To generate necessary random bit sequences, Chaotic logistic and Tent maps were used.

Wang et al. [9] developed a threshold approach to generate the best bit-budget for the image waveform based on the 'Tchebichefpsychovisual' threshold. This bit-budget was designed to restore most of the quantization tables in image compression. The study results showed that the developed model can better improve the visual characteristics of the image result. The consistency of the visual image produces fewer objects and pixel deformation of the image [10]. A community of bits-budgets therefore provides an excellent creation with reduced bit lengths in image quality [11]. Finally, the method adopted was tested and positive research results were obtained by distinguishing between conventional systems.

Zhang et al. [12] introduced a new method to measure the finer limitations of fractal encoding to minimize their computational complication. The scaling constraint has been uncomplicated but proficiently calculated that rewards all the characteristics required to achieve convergence. It makes an uncomplicated distribution of two integers to replace the expensive process. In addition to their conventional models a customized HV block partition system and many new ways of developing an encoding and decoding cycle were adopted. From the analysis results, better output in a reduced period was verified in the technique used, similar to conventional models of fractal-dependent image compression.

Hayder et al. [13] employed an improved Embedded Zerotree Wavelet EZW to achieve better compression rates and PSNR to achieve loss-free image compression accordingly. The method adopted uses a novel symbolic map, symbolically more effectively, to minimize the count scanning and symbol duplicates of prevailing EZW. The adopt model was further developed to achieve a scalable image coding by efficient deployment of the interdependence of coloured planes. Simulation findings demonstrate, eventually, that the scheme adopted has support of both subjective and objective principles [14] for different compression schemes over the standard and other enhanced models.

In order to create a better image crypt method, Fathi et al. [15] have used vector quantization. The method is focused on vector quantization, one of the most common techniques of image compression. In vector quantization (VQ), the images are broken down into vectors and vector-by-vector sequentially encoded. The aims of this approach are to build a high-security picture crypto framework and reduce encryption and decryption algorithm computational complexity.

## III. Proposed Model

In the field of image processing, immense amount of data need be considered and handled [16]. The overall compression issue is that the amount of information required to represent a digital image is reduced and the elimination of spatial and psycho-visual redundancies is the basis of the process of reduction [17]. The compression would be a waste if the re-constructed image from the compressed image is the same as the original. The way the image size can be obtained without greatly affecting its quality is image compression [18]. Uncompressed images have a higher time complexity than compressed images during transmission and reception [19]. To protect images against unauthorized access, such as scratching, intercepting and hacking, image protection is essential [20]. The image needs to be encrypted to provide security which leaves the picture unreadable and unmodified. Picture encryption [21] is a process by which images are encrypted and decrypted during transmission [22].

Implementing various safety measures at various levels is very necessary in order to provide information as a signal in the form of an image [23]. In the proposed model the image is initially segmented into sub images and then on sub images segmentation is performed and then pixel extraction is performed. The pixels extracted from the image are interchanged and then compression technique is applied. The compression technique will undergo encryption process for

securing the image during data transmission. The proposed work framework is depicted in Fig. 1.

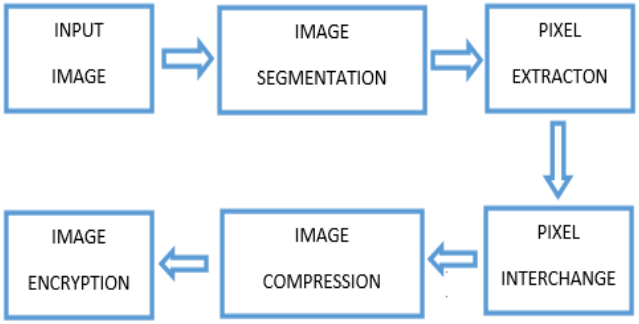



Fig. 1. Proposed Model Framework.

The process of the Image Segmentation based Compression Model with Pixel Interchange Encryption (ISbCPIE) Model is detailed in the algorithm.

**Algorithm ISbCPIE**

{

Input: Image $I_N$

Output: Encrypted Image $E(I_N)$

**Step 1:** Initially the image is provided as input which undergoes image segmentation. The sub image is again segmented further to accurately detect the pixels within the boundary and exact edges are detected. The process of segmentation is performed as

$$l_N(l_x, l_y) = \sqrt{\sum_{c=l_i}^{l_N} I(pix(i)) + (T - l_i(x-y))^2 \times pix_l^{I[l_i,l_j]} + \theta(I(x,y))} \quad (1)$$

Here $I_N$ refers the image considered, x and y refers the adjacent pixels, pix(i) refers the extracted pixel, T is the maximum threshold value of the pixel intensity. $\theta$ refers the angle of the image. The image segmentation results in generation of sub images and again the sub image will undergo segmentation for accurate pixel extraction by considering the boundaries and edges.

**Step 2:** The process of arranging the images in the sequence for performing pixel extraction is performed as

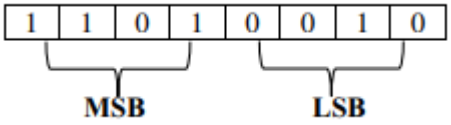
$$Sq(I(x,y)) = \sum_i pix(I(i) + I_N \theta_{i,j} + \theta(pix(i)) + exp\left(\frac{-(pix_j(i) - pix_i(j))^{\theta}}{\left(\frac{2\theta^2}{N}\right)}\right) \quad (2)$$

**Step 3:** After arranging the images in the sequence order, the pixels need to be extracted by considering the edges and boundaries. For a X*Y image, the first X bits are used to calculate the initial location of the permissible random pixel. In calculating the target location of the selected pixel, the last Y bits are used. It is repeated in X*Y numbers, ensuring that all the locations of the pixels are allowed. The next position available is chosen if a pixel is already allowed in the initial position or a target position is already filled. The pixels are extracted using the equation:

$$pix(I(x,y)) = \frac{\left(\sum_{i=1}^{h}\sum_{j=1}^{w}\left(x_{ij} - \overline{X}\right)\left(y_{ij} - \overline{Y}\right)\right) + \sum_{i=1}^{N} Min(Sq(i)) - Max(pix(I(x,y)))}{\sqrt{\left(\sum_{i=1}^{h}\sum_{j=1}^{w}\left(x_{ij} - \overline{X}\right)^2\right)\left(\sum_{i=1}^{h}\sum_{j=1}^{w}\left(y_{ij} - \overline{Y}\right)^2\right)}} \quad (3)$$

X,Y are the average values for original image pixels, and h and w are the height and width of the image, where x,y are adjacent image pixels with in the boundary, respectively.

**Step 4:** An image is defined as a two-dimensional I(x, y) function, where x and y are pairs of coordinates. The I(x,y) is a value called grayscale, which is the light intensity of pixels in coordinates (x,y). A pixel value can be translated to 8 binary numbers (bits). Four digits of the first are referred to as the LSB, which does not change the picture dramatically when changing value in this position. The second is called a 4 digit MSB, with an essential effect on the image by changing value in this place. The below representation shows the place of a bit value of a pixel value.




**Step 5:**The correlation coefficient of the image specifies how the relationship of the pixels adjacent to each other is calculated. The formula to calculate the correlation coefficient of the image is:

$$cc(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad cc(y) = \frac{1}{N}\sum_{i=1}^{N} y_i$$

$$CC = \frac{\sum_{i=1}^{N} \frac{x_i - cc(x)}{y_i - cc(y)} + \theta(I(x,y)) - \min(pix(I(x,y)))}{\sqrt{\sum_{i=1}^{N}(x_i - cc(x))^2}\ \sqrt{\sum_{i=1}^{N}(y_i - cc(y))^2}} \quad (4)$$

Here $x_i$, $y_i$ are the adjacent pixels of plain sub image at i position with angle $\theta$and N indicates the pixels count in the sub image.

**Step 6:** The pixels between cc(x) and cc(y) are exchanged by

$$\sum_{i=1}^{N} I\begin{pmatrix} x \\ y \end{pmatrix} = \sum_i I\begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix}\begin{pmatrix} y \\ x \end{pmatrix} + \begin{pmatrix} p-y & p+x \\ q & x+y \end{pmatrix} \text{mod CC.}$$

$$PiM\begin{pmatrix} x \\ y \end{pmatrix} = \sum_{i=1}^{N} I\begin{pmatrix} x+(p-1+y) \\ y+(q-1+x) \end{pmatrix} \quad (5)$$

where, p and q are the adjacent boundaries of sub images extracted from an image.

**Step 7:** After pixel interchange is performed, the compression technique is applied on the pixel interchange matrix that is performed as

$$Si_{i,j}(I_N(i)) = \sum_{i=1}^{N} \sum_{i=1}^{N} I\begin{pmatrix} x \\ y \end{pmatrix} + pix(i,j) + \left\{\frac{\left||i_j - CC(x)_i|\right|}{\left||j_j - CC(x)_y|\right|}\right\}^{*\theta} \quad (6)$$

$$Comp(I(X,Y)) = \sum_{i,j=0}^{N} \frac{pix(i,j) + \theta\left(Si_{i,j}(I_N(i))\right) - \sum_{i,j=0}^{N-1} pix_{i,j}(i-j)^2}{(i-j)^2 + CC(x) - CC(y)} \quad (7)$$

**Step 8:** After the compression is completed the encryption technique is applied on the compressed image for providing security to the image during data transmission. The process of performing encryption undergoes several phases including key generation and then encryption. To generate the key the process involves in considering two random numbers as:

$$p = \left(\sum_{i=1}^{H}\sum_{j=1}^{W} Sq(I(x,y))\right) \bmod CC(x),$$

$$q = \left(\sum_{i=1}^{H}\sum_{j=1}^{w} Comp(i_i(x,y))\right) \bmod CC(y).$$

After calculating the p and q values, the key is calculated as

$$TempK(i) = \sum_{I=1} \sum_{j=i-1} p_j^l * p_i^N + \sum_{i,j \in N} Si_{i,j}\left(I_N(i)\right) + \sum_{i=1} \log pix(x, y_n = 0 | X : H + Y : W) \quad (8)$$

$$PrivK(i) = \sum_{I=1}^{N} TempK(i) + \sum_{i}^{N} \mathrm{CC(x)} \log S_{in} - \sum_{i}^{N} (1 - \mathrm{N} + \mathrm{CC(y)}) \log(1 - S_i) \quad (9)$$

**Step 9:** The image encryption technique is applied on the pixel interchanged matrix as:

T1= $PiM\begin{pmatrix} x \\ y \end{pmatrix} \oplus$ p*q

T2= T1<<p $\oplus PrivK(i)$

T3= T2>>q $\oplus$T1>>p $\oplus PrivK(i)$-q

T4= CC(x) + leftcirshif(T3) +CC(y) $\oplus TempK(i) \oplus PrivK(i)$+mod(p,q)

T5= T4>>Th$\oplus$ T2<<Th $\oplus$ ($PrivK(i)$+Th)

}

The image after performing the image pixel extraction, compression and encryption, the encrypted image can be stored in cloud as the data is very secured.

## IV. Result

The proposed model is implemented in ANACONDA SPYDER for performing image segmentation, pixel extraction and pixel interchange to perform encryption. Numerous security analysis tests were performed in order to determine the efficiency of the suggested methodology on images. The images are considered from the links https://www.kaggle.com/puneet6060/intel-image-classification?select=seg_train and https://data.mendeley.com/datasets/3hfzp6vwkm/3. For every single image, each pixel in horizontal, vertical or diagonal directions is highly correlated with its neighboring pixels. An attacker may use this connection to carry out statistical assaults. The cryptographic algorithm should therefore construct an encrypted picture with a low pixel correlation to resist such statistical attacks. In the three directions referenced, 2,800 pairs of adjacent pixels are chosen randomly in two pictures to determine a correlation in both the single-picture and cipher-image directions. The proposed model is evaluated by considering several parameters like image segmentation time levels, pixel extraction time levels, compression time levels, pixel interchange accuracy, Encryption Accuracy, Encryption Time Levels, Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The proposed model provides a secured platform for transmitting the images in the network.

For gray images with 256 levels, where each gray level is considered to be equi-probable, its entropy will be 8sh (or bits). An image encryption algorithm should preferably offer an encrypted image with equipment that is gray. The entropy values for the considered image when applied on different algorithms are indicated in the Table I.

TABLE I. Entropy Values

| Algorithm Applied | Entropy (sh) |
|---|---|
| Proposed ISbCPIE | 8.24 |
| Chaotic Cryptography (CC) [3] | 7.86 |
| Block Cryptosystem based on Iterating a Chaotic Map (BCICM) [17] | 7.67 |
| Chaos-based PWL Memristor (CPWLM) [18] | 7.52 |

The proposed ISbCPIE model is compared with the traditional Chaotic Cryptography (CC), Chaos-based PWL Memristor, Block Cryptosystem based on Iterating a Chaotic Map (BCICM), Chaos-based PWL Memristor (CPWLM) models. The proposed model initially performs image segmentation and then again each segmented image is segmented for accurate pixel extraction with exact edges and boundary values. The image segmentation time values are depicted in Fig. 2.

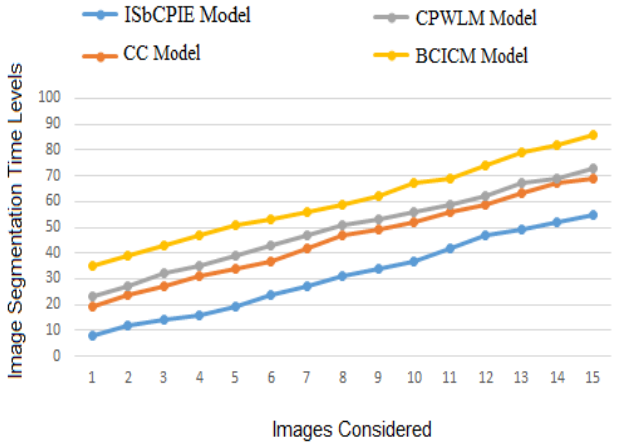



Fig. 2. Image Segmentation Time Levels.

The image considered will undergo segmentation and then from each sub image, pixel extraction is performed for considering the values to perform multiple operations like compression and applying cryptography techniques. The Pixel extraction time levels of the proposed and traditional models are depicted in Fig. 3.

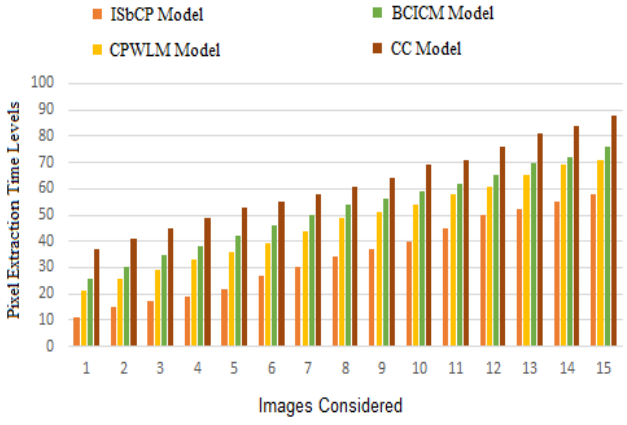



Fig. 3. Pixel Extraction Time Levels.

The extracted pixels undergo the process of interchanging the pixels positions to a specific position for providing the security levels during image transmission. The pixel interchange accuracy levels of the proposed and existing models are indicated in Fig. 4.

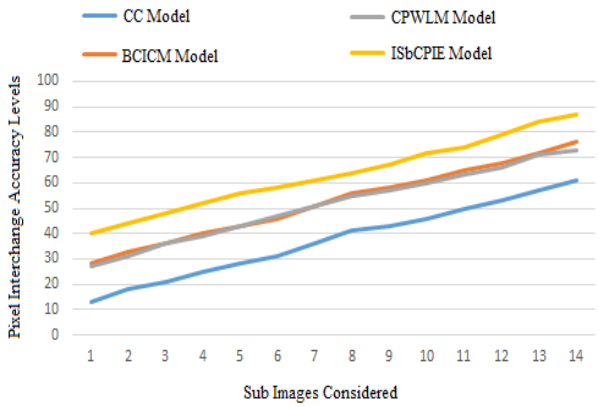



Fig. 4. Pixel Interchange Accuracy.

The pixel interchanging model allows the users to increase the security levels in hiding the image from the attackers. The image pixels which are interchanged are compressed to reduce the size and for quick data transmission. The Image pixel compression time levels are indicated in the Fig. 5.

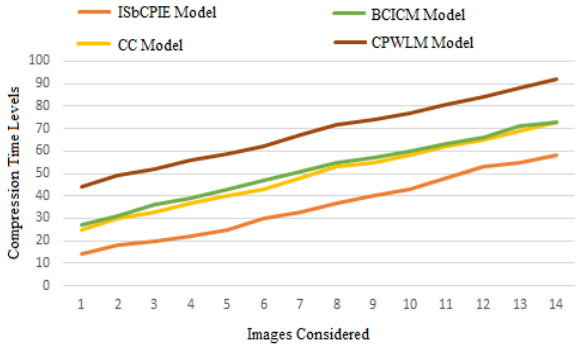



Fig. 5. Compression Time Levels.

The original image is considered as input and then it undergoes image segmentation. All image segments undergo pixel extraction and pixel bit interchange for improving the security levels during data transmission. The compression technique is applied on the image segments and then encryption is performed. The Original image and encrypted image is represented in Fig. 6.

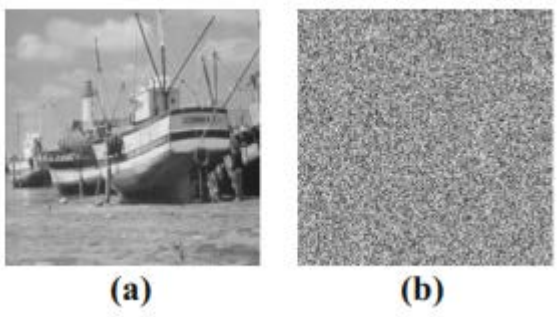



Fig. 6. (a) Original Image (b) Encrypted Image.

The proposed encryption model is effective and the encryption accuracy of the proposed model is compared with the traditional models. The encryption accuracy levels are indicated in Fig. 7.

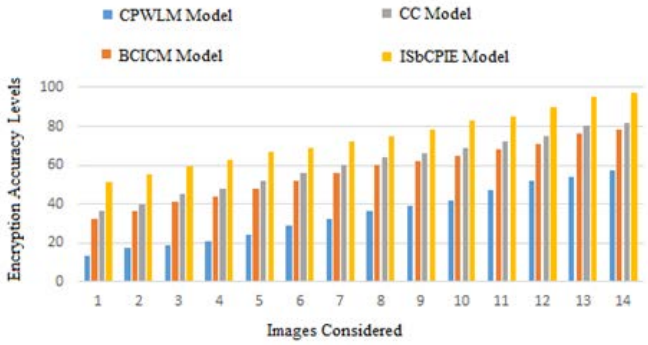



Fig. 7. Encryption Accuracy.

The time for performing encryption in the proposed model is low when compared to traditional methods. The encryption time levels are indicated in Fig. 8. The Table II illustrates the time levels of performing encryption on various image sizes.

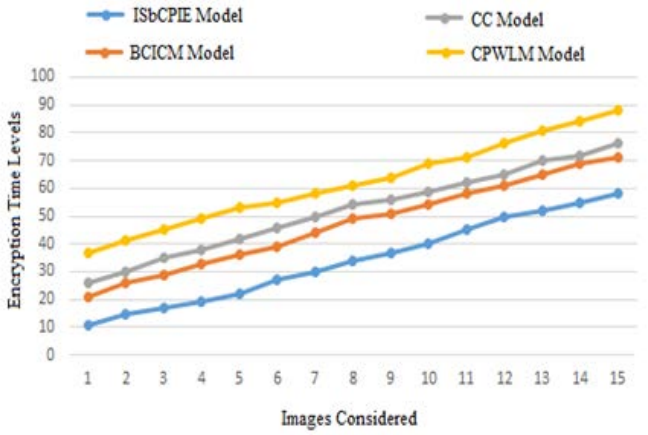



Fig. 8. Encryption Time Levels.

TABLE II. TIME FOR ENCRYPTION FOR VARIOUS PICTURE SIZES

| Image size | Average Pixel Interchange Time (ms)-Proposed Model | Average Pixel Interchange Time (ms)-Existing Model | Average Encryption Time (ms)-Proposed Model | Average Encryption Time (ms)-Existing Model |
|---|---|---|---|---|
| 256 x 256 | 4 | 9 | 5 | 12 |
| 512 x 512 | 12 | 17 | 15 | 23 |
| 1024 x 1024 | 43 | 91 | 63 | 97 |

The cryptographic value of the proposed image encryption structure is calculated by measuring the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The process of calculating MSE and PSNR are:

$$MSE = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} \left(a_{ij} - b_{ij}\right)^2$$

The mean square error (MSE) representation of the proposed and the existing models are represented in Fig. 9.

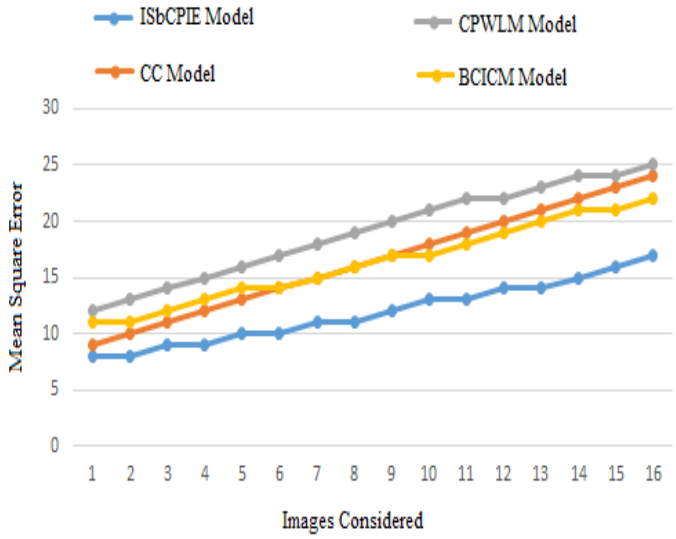



Fig. 9. Mean Square Error.

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right)$$

The Peak Signal-to-Noise Ratio (PSNR) representation of the proposed and the existing models are represented in Fig. 10.

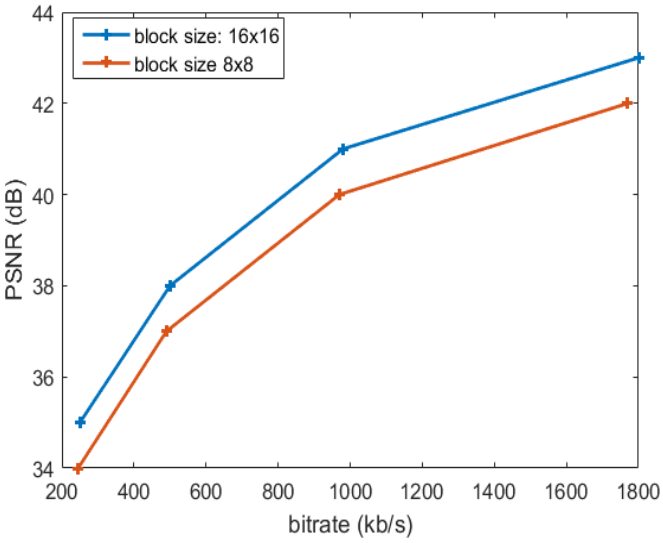



Fig. 10. PSNR Representation.

## V. CONCLUSION

Digital files are communicated at any moment, on any computer and with everyone on the planet. In this digital era, lakhs of users are depending on digital communication and seek to communicate efficiently and safely. There is a continuous improvement in communication with stronger demands on productivity and protection, where effectiveness is data compression and security is encryption. Digital communication can be based on a structure which is expressed in two heterogeneous and often contradictory operations, but which must be applied to the original file in order to ensure efficiency and safety. The enemy of compression is randomness, but on the other hand encryption needs to add a randomness to digital data to offer protection. These two operations are compression and encrypting. The proposed algorithm focuses on the simultaneous compression and encryption of random pixel interchange model. Divide the image into the blocks of equal size in the proposed process, and every block is again subdivided into frequencies and then performed with pixel interchange and then encrypts every substructure and encapsulates the respective sub-block in one block. For all sub-blocks and blocks, the same process is performed. Random pixel exchange between compression and encryption blocks is performed. The encrypted data can be securely stored in cloud. The algorithm proposed improves the flexibility and robustness of image protection. The proposed model accuracy and security levels are also high when compared to traditional models. In future the key generation techniques need to be concentrated more to enhance the security levels of data during transmission. In future, the computational complexity levels of the proposed model can be reduced by the usage of feature reduction model to improve the accuracy levels.

## REFERENCES

[1] Ma, S.W.; Zhang, X.; Jia, C.; Zhao, Z.; Wang, S.; Wanga, S. Image and Video Compression with Neural Networks: A Review. IEEE Trans. Circuits Syst. Video Technol. 2019. [Google Scholar] [CrossRef].

[2] Aqeel-ur-Rehman XL, Hahsmi MA, Haider R (2018) An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik 153:117–134.

[3] Jallouli O, Assad SE, Chetto M, Lozi R (2018) Design and analysis of two stream ciphers based on chaotic coupling and multiplexing techniques. Multimed Tools Appl 77:13391–13417 21.

[4] Klinger E, Starkweather D (2018) pHash–the open source perceptual hash library. Available: www.phash.org.

[5] Xu M, Tian Z (2018) A novel image encryption algorithm based on self-orthogonal Latin squares. Optik 171:891–903 43. Zhang Y, Tang Y (2018) A plaintext-related image encryption algorithm based on chaos. Multimed Tools Appl 77:6647–6669.

[6] Jiang, F.; Tao, W.; Liu, S.H.; Ren, J.; Guo, X.; Zhao, D.B. An end-to-end compression framework based on convolutional neural networks. IEEE Trans. Circuits Syst. Video Technol. 2018, 28, 3007–3018.

[7] Luo, S.H.; Yang, Y.Z.; Song, M.L. DeepSIC: Deep Semantic Image Compression. In Proceedings of the International Conference on Neural Information Processing (ICONIP) (2018), Siem Reap, Cambodia, 13–16 December 2018. [Google Scholar].

[8] Kumari M, Gupta S (2018) A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher. 3D Res 9:10.

[9] Wang X, Zhu X, Zhang Y (2018) An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access 6:23733–23746.

[10] Kaur M, Kumar V (2018) Adaptive differential evolution-based Lorenz chaotic system for image encryption. Arab J SciEng 43(12):8127–8144.

[11] E. Setyaningsih and R. Wardoyo, "Review of image compression and encryption techniques," International Journal of Advanced Computer Science and Applications, vol. 8, no. 2, 2017.View at: Publisher Site | Google Scholar.

[12] Y. Zhang, B. Xu, and N. Zhou, "A novel image compression–encryption hybrid algorithm based on the analysis sparse representation," Optics Communications, vol. 392, pp. 223–233, 2017.

[13] Z. Hayder, X. He, and M. Salzmann, "Boundary-aware instance segmentation," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 5696–5704.

[14] M. Bai and R. Urtasun, "Deep watershed transform for instance segmentation," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 5221–5229.

[15] A. Fathi, Z. Wojna, V. Rathod, P. Wang, H. O. Song, S. Guadarrama, and K. P. Murphy, "Semantic instance segmentation via deep metric learning," arXiv preprint arXiv:1703.10277, 2017.

[16] L.-C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, "Deeplab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected crfs," IEEE transactions on pattern analysis and machine intelligence, vol. 40, no. 4, pp. 834–848, 2017.

[17] Tao Xiang, Xiaofeng Liao, Guoping Tang, Yong Chen, Kwok-wo Wong, A novel block cryptosystem based on iterating a chaotic map, Physics Letters A, Volume 349, Issues 1–4, 2006, Pages 109-115, ISSN 0375-9601.

[18] Lin, Zhaohui & Wang, Hongxia. (2010). Efficient Image Encryption Using a Chaos-based PWL Memristor. IETE Technical Review. 27. 10.4103/0256-4602.64605.

[19] Belazi A, Khan M, El-Latif AAA (2017) Belghith. Efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption Nonlinear Dyn 88:337–362.

[20] Ashur T, Dunkelman O, Luykx A (2017) Boosting authenticated encryption robustness with minimal modifications. Springer International Publishing, Cham, p 3–33.

[21] Xiao D, Chang Y, Xiang T, Bai S (2017) A watermarking algorithm in encrypted image based on compressive sensing with high quality image reconstruction and watermark performance. Multimed Tools Appl 76:9265–9296.

[22] Zhou, B.L.; Khosla, A.; Lapedriza, A.; Oliva, A.; Torralba, A. Learning deep features for discriminative localization. In Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 26 June–1 July 2016; pp. 2921–2929. [Google Scholar].

[23] Radford, A.; Metz, L.; Chintala, S. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks. Available online: http://arxiv.org/pdf/1511.06434.pdf (accessed on 7 January 2016).