IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 39, No. 1, February, 2022, pp. 195-203
Journal homepage: http://iieta.org/journals/ts

An Image Decompression Model with Reversible Pixel Interchange Decryption Model Using Data Deduplication

Naga Raju Hari Manikyam*, Munisamy Shyamala Devi

CSE Department, VelTech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai 600062, Tamilnadu, India

Corresponding Author Email: vtd521@veltech.edu.in

https://doi.org/10.18280/ts.390120

Received: 28 June 2021
Accepted: 26 December 2021

Keywords:
data deduplication, image decompression, reversible pixel interchange, storage provider, decryption

ABSTRACT

The images may or may not be confidential if communications occur via images. But it becomes complicated when we want to convey a picture, which only the sender and the recipient must know. Since data that have been sent during transmission can be lost or an individual may hack and misuse this picture. Safety of the data is important in such scenarios. In order to reduce storage space and costs, imaging deduplication (DD) technology is proposed. The concept of convergent encryption and decryption was suggested to protect the confidentiality of the image. The deduplication scheme encrypts/recodes an image with a convergent encryption/decryption key obtained from computing the hash value of the content of the image. Implementing DD over encrypted/decrypted data is a major challenge to optimize storage efficiently in a highly secured way in an integrated storage and computer environment. The original image is segmented into blocks of same size during the initial step, and sub classification is performed for accurate image extraction within the limits. The pixels of neighboring sub blocks are swapped using a random matrix. Following that, each pixel is randomly exchanged for neighboring blocks using a random matrix, and each block is encrypted using the suggested function before being sent to the receiver. In this manuscript, an Image Decompression Model with Reversible Pixel Interchange Decryption model using Data Deduplication (IDRPID-DD) is introduced that provides security during storage and data transmission. The proposed model is compared with the traditional methods and the results show that the proposed model deduplication identification and eradication levels are high and the proposed decryption model is strong.

1. INTRODUCTION

The great evolution of service providers has drawn more and more attention to the application of information and communication on the Internet. Storage service providers are modern computing paradigm with dynamic extension ability to access computing resources and services via the Internet on-demand [1]. It receives a great deal of attention due to its unique methodology and its evolving academic and industrial business storage model [2]. Network backups, however, face an immense challenge with the exponential increase in data, the mass of information storage and the application demands for high-data availability [3]. However, we get knowledge and the kind of scientific experiments that are produced daily. According to IDC's (international data company) resent analysis states that, 1315 EB data were generated worldwide in 2020 and each individual has 69 GB of data on earth. The number of data generated worldwide is nearly 8800 EB, 10 times the amount in 2010. The world's data volume is projected to exceed 50 trillion GB by 2022 [4].

Data deduplication technology has recently been proposed for the above situation. Technology for Data Deduplication is a lossless technology for data compression focused primarily on the concept of deletion [5]. This technology could reduce data transfer and storage costs. Especially in the picture files in the social network, a message is often sent more than a thousand times soon to a public. Iconic pictures are sometimes replicated too. If such store operations still occur, storage space would surely be wasteful [6]. The problem cannot be solved simply by increasing storage capacity. Image deduplication to the social network must be applied [7].

When it relates to applications and utilisation of the network in online banking, retail, social networking, and other areas, today's society is more reliant on network communication. The rapid advancement of networking technology leads to the exchange of a large volume of information. As a result, data security is required while communicating confidential information. Encryption and decryption algorithms are utilised, with encryption scrambling plain text into cypher text and decryption scrambling plain text into cypher text. A secret key or code is used to encrypt and decode the data. An intruder without the key will be unable to decrypt the messages. As a result, cryptography is essential for information security. There are several types of cryptography like symmetric and asymmetric cryptography. The use of a single key both for encryption / decryption is known as symmetric key cryptography. In public key cryptography, one key serves as the public key that is used for encryption and another serves as the private key for decryption.

The concept of convergent encryption was proposed to protect the confidentiality of the image. The image is encrypted/decoded in the deduplication scheme by means of

the convergence encryption/decryption key that comes from computing the image contents hash value [8]. This means that the same image copies produce the same cypher text to enable a deduplication on cipher texts by the cloud storage server. In addition, image users use the attribute-based encryption system to share pictures with friends by setting privileges of access [9]. Data and information exchange today generally takes place through insecure public networks. The use of insecure means of communication, such as social media, is highly susceptible to information misuse by third parties [10]. It is vital, therefore, that data, including images sent through unsecured channels, is kept confidential [11].

The exchange of image data via public networks has two main problems. First of all, because of the need for good image quality the size of image data is growing [12]. The transmission of image data takes longer. The compression method can be applied to the data before sending this problem. The second issue is the poor safety of image data because it distributes image data on a public network [13, 14]. This issue can be resolved with the encryption of the message. Compression and encryption is rather interrelated and communicated [15]. Data compression takes place by reducing image data redundancy, while data encryption produces a high security level if the image data redundancy is poor. Compression and encryption are therefore also done in conjunction with smaller dimensions, better quality, quick transmission and high safety [16]. Various techniques have been developed with their benefits and drawbacks for combining compression and encryption methods based on sequence processes [17].

Information and communication technologies are evolving more rapidly and huge data is transmitted through a highly secure communication medium. Even confidential or hidden information should be kept safe from misuse and protected. Information security is required for various applications such as information storage, information processing, security for customers, satellite image security, classified video conferencing, telemedicine, military information and many other applications [18]. Confidential contact in social life has long been a common practice. Because information may, however, be shared electronically, the public domain is exposed and interceptions are inevitable [19]. Cryptography is called a scientific method in order to meet the demands for defense. The cryptosystem is also used in cryptography, and is often known as the cipher [20]. The main subject of encryption/decryption is to alter the message that only an approved recipient can identify in his original message.

Encryption is a widely used technique and practice in digital information security systems. Digital information can be secured if the encryption method's security and dependability are strong enough. Since digital picture encryption technology and methods are critical to digital image security protection, this research is essential. However, the requirements for text encryption drive the development of encryption technology and systems [21]. At the moment, the more popular encryption system cannot obtain better results in terms of digital image compatibility and encryption quality. When using text-encryption techniques, cryptographic algorithms that directly use two-dimensional data sets suffer challenges of inefficiency, low technical feasibility, and low security. Encrypting digital images in a network context requires research into a cryptographic technique or encryption method that is appropriate for this purpose.

Unreadable, encrypted transformed data is returned to its original format by a decryption technique that works in the opposite direction to that of encryption. In a decryption method, the machine extracts and transforms the cipher data into texts and images which can be read and understood easily. Manual, automatic, or key/password decoding are all common methods of decoding. The ubiquitous usage of pattern recognition, face detection, image restoration, and picture matching across a variety of fields makes it challenging to apply image encryption and decryption techniques.

As a universal data redundancy elimination technology, the data deduplication is considered. DD classifies identical data mostly, stores copies of the data and replaces with undirected references other similar copies, rather than with a complete copy. Some commonly used models are Chunking, Hashing and Matching Hashes to Redundancy [22]. The method of chunking splits a file into several smaller files called chunks. By comparing it with all incoming duplicate identification chunks, the chunk deduplication approach improves the storage of unique chunks [23]. The owner does not guarantee data protection in remote storage systems until data is uploaded to the storage. Deduplication is imperative for efficient storage at the same time. In order to ensure optimised and safe storage, encryption and deduplication should therefore be performed simultaneously. DD could be used for a certain amount of time in files or programmes. The key used to encrypt and decrypt the data is generated and will be resistant to further attempts.

2. LITERATURE SURVEY

Wang et al. [1] provided a stable user-revocation deduplication system. The '3' framework includes: upload, cancel, and download stages. A privilege-centred encryption technique over convergent-encryption executes the supported system. Li et al. [2] suggested, a model in which users need not have to handle keys, but instead spread convergent key actions safely over several servers. Duplication file-level eradicated storage of redundant files and deduplication at block-level divided the files into smaller blocks or fixed blocks, and removed the storage of all redundant blocks.

A new algorithm has been submitted by Zhang [5] that works on two things: compression and encryption of binary and gray-scale images. SCAN patterns generated by SCAN methodology that is used to compress and encrypt schemes. The SCAN is a systematic 2D access methodology based on language that generates a variety of scanning paths or space filler curves.

On the server side of the encrypted data Hamdi et al. [7] recommended a deduplication framework. It allows the Cloud Server to manage access to the external data because ownership of the secured distribution of main groups has changed dynamically and has randomised CEs. It can alert revoked users of data leakage, even if they used to possess the data or cloud storage. The device ensures data integrity such as the assault on tag incoherence. The results of the efficiency estimation showed that, while the extra charge for calculations was negligible, the scheme is nearly as effective as the old framework.

The file-level deduplication technique is to delete the same file, to save data storage space. A hash function is used to calculate a hash value for each file. Any two files with the same hash value are the same file. This approach is used, EMC Center [9] systems. The deduplication-based technique is to

remove the same database block in order to reduce the storage space. The approach is to split a file into certain fingerprint blocks and uses Hash functions to calculate the hash value called a fingerprint block. Two data blocks are classified as duplicate data blocks with the same fingerprint block.

Deduplication technology may be divided into online deduplication and deduplication after depilation based on the deduplication deletion period. Online deduction is needed to remove the duplicate data prior to storage. A unique copy is always saved by the storage provider. Additional storage buffer for post-6 processing deduplication is required to remove repeated data. The deduction can be split into customer deduplication and operation deduplication, based on the deduction site. Clients are checked and deleted before uploading the data copy to the cloud server. Service deduplication is performed through duplicate data verification and deletion using the cloud server resource.

However, videos are larger than text, multi-mediated data like photographs. This increases the importance of picture deduplication. This area has been taken care and a new image deduplication model is proposed by Aqeel-ur-Rehman et al. [11]. Before we download the photos to the server, we have to manage them in general. Compression technique somehow saves the capacity of the cloud storage, but root deduction addresses this. The method of obtaining encrypted images was proposed by Zhen et al. [14], which inputs the image data to AES Encryption. The encrypted picture is used to access the original image as input for AES Decryption. In this document, 128 bit AES is used to encrypt and decrypt images which have been synthesised and simulated with Xilinx ISE 12,4 tool in the Spartan-6 FPGA (XC6SLX25) family, with high speed Hardware Description Language integrated system (VHDL).

Duan et al. [16] proposed an image encryption approach, however shifting is the most important part of this technique. The first step is picture encryption, which involves dividing the image into blocks and then randomly permuting those blocks. The encryption is made more secure by applying additional permutation based on a random number. After encryption, a key is generated by combining the values used to encrypt the data. The secret image is used to produce shares in the next phase, which is the identification procedure.

Image encryption can benefit from the qualities of the chaos-based approach. A feature of chaos-based techniques is their sensitivity to the starting conditions, which means that even the smallest change in the initial conditions can have a significant impact on the system's behaviour. Encryption relies on a variety of chaotic maps [17]. A chaotic map is a function that depicts the disordered organisation of an area. Random numbers are generated using chaotic maps. Some of the most important chaotic maps include the logistic map and the Renyi map. The series of integers that can be used as a key to encrypt an image is generated by chaotic systems. The sensitivity to beginning conditions is one of the features of chaotic systems that is necessary for picture encryption and decryption [18].

Images can be encrypted using a big pseudorandom permutation created from small permutation matrices generated from chaotic maps, according to Kumari et al. [19]. Using the permutation matrix, the randomness of chaos may be efficiently dispersed into encrypted images. After creating an initial tiny matrix using a chaotic logistic map, they apply the chaotic image cypher. The authors built a big permutation matrix from a series of smaller ones. Using the permutation matrix, the image's pixel values were rearranged. Liu et al. [20] used two chaotic systems to obfuscate the relationship between both the plain-image and cipher-image by employing a new picture total shuffling matrix that shuffles the positions of each image pixel.

3. PROPOSED MODEL

Deduplication decreases storage space as it enables the retention of only one data instance and eliminates all duplicate copies of the data files and replaces all redundant files by a pointer indicating the unique data instance [24]. Data Replication technology optimises the storage providers' computing capacity to use disc space efficiently. Another advantage of deduplication is that the duplicate data copies are not transmitted and upload bandwidth is not saved when performed at source [25]. The deduction of data helps to accommodate increased data volume and decreases operating costs and storage costs. The image deduplication process is represented in Figure 1.

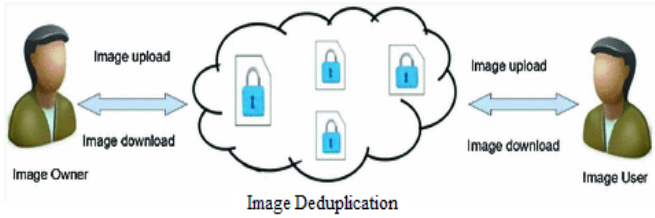

Figure 1. Image deduplication process

Image matching is a tool used either to describe the entire image with global features which can describe a complete picture by only one vector or to concentrate on important image information that is stronger. We must deal with the contents and obtain information from these two methods in order to implement the two, which means that both methods take time to handle images and that they require hardware capable of acquiring these features efficiently [26]. This leads us to the fact that mobile device extraction takes a lot of time, random memory, thus increasing battery consumption, thus affecting the user's everyday use.

Matching of images is one of the main tasks for removing duplicated files. Most of the functions are chosen for the reduction of the time of the computer, and the image is the same as the input file in a database. In some applications, matching is one of the essential processes. Mobile technology has been a hub of science and everyday life in the past ten years. The process of Image Decompression Model with Reversible Pixel Interchange Decryption model using Data Deduplication (IDRPID-DD) is detailed in the algorithm.

Algorithm IDRPID-DD

{

Input: Encrypted Image $E(I_N)$

Output: Decrypted Image $D(I_N)$

Step-1: The encrypted image is provided as input to store the data in cloud environment or any memory location. The image uploaded has to be verified with duplication so that memory wastage can be reduced. If the same image is uploaded for multiple times, it leads to memory wastage and deduplication model has to avoid it for reducing memory wastage. The input encrypted image is analysed as if any duplicate is identified, its hash value is stored instead of

complete image to avoid deduplication. The encrypted image is compared with the existing images and the duplication status DS is identified as

$$DS(x, y, f) = \sum_{i=o}^{x}\sum_{j=0}^{y}\left[\frac{getdata(E(I_N)*(x,y)) + \forall(Mem(I_N)}{Tot(E(I_N)) + \theta} + \theta(I_N)\right] \quad (1)$$

$$DSindex(x,y) = \begin{cases} 1, & E(I_N) = Mem(I_N) \\ 0, & E(I_N) \neq Mem(I_N) \end{cases}$$

Here f is the flag value which ins increased when the image match is found. The flag value indicates the number of duplicate entities identified.

If *DSindex* is triggered as 0, then the image is uploaded in the cloud environment or in any memory unit and then step-2 is initiated. If *DSindex* is triggered as 1, then it represents that match is found and then its hash value is calculated and stored in its respective existing memory header for reference. The hash value HV is extracted and stored as

$$HV(E(I(i,j)))_N = \frac{\sum_{x=1}^{N}(Hash(E(I))_{x,y}^{N})\, x_j}{\sum_{y=1}^{N} \forall(Mem(I_N) + DSindex(x,y)} \quad (2)$$

The hash value is stored in the memory unit as

$$Mem(E(I_N)) = \left(\frac{\Sigma\overline{HV(E(I(i,j)))} + \forall(Mem(HV_N) + Th}{\Sigma\max(HV(I(x,y)))}\right. \quad (3)$$

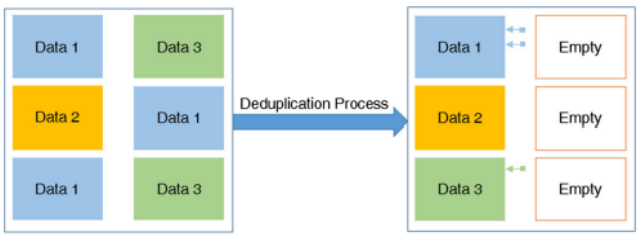

Figure 2. Image deduplication

The duplicate images are removed to save memory and to reduce the complexity of the model. The deduplication process is depicted in Figure 2.

Step-2: The keys are calculated for performing the decryption. The private key is calculated by considering the 2 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

$$TempK(i) = \sum_{I=1}\sum_{j=i-1} p_j^l * p_i^N + \sum_{i,j\in N} Si_{i,j}(I_N(i)) + \sum_{i=1} \log pix(x, y_n = 0|X:H+Y:W) \quad (4)$$

$$PrivK(i) = \sum_{I=1} TempK(i) + \sum_{i}^{N} \mathrm{CC(x)} \log S_{in} - \sum_{i}^{N} (1 - \mathrm{N} + \mathrm{CC(y)}) \log(1 - S_i) \quad (5)$$

Step-3: The image when accessed by any new user performs decryption operation that is performed as

D1=$PiM\begin{pmatrix}x\\y\end{pmatrix}$& p-q

D2= T1>>p$\oplus PrivK(i)$>>D1

D3=T2>>q &T1<<p $\oplus PrivK(i)$+q<<D2

D4=CC(x)-rightcirshif(T3)-CC(y)&$TempK(i)$&$PrivK(i)$-mod(p,q)

D5=T4<<Th& Th>>Th | ($PrivK(i)$-Th)

Step-4: After the image is decrypted, the image will be in the compression format. The image decompression will be performed as

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

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

Step-5: The pixels range from cc(x) to cc(y) are interchanges as $\Sigma_{i=1}^{N} I\begin{pmatrix}x\\y\end{pmatrix} = \Sigma_i I\begin{pmatrix}1+pq & q\\ p & 1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} - \begin{pmatrix}x-y & y\\ p-x & y-p\end{pmatrix}$ mod CC.

$$PiM\begin{pmatrix}x\\y\end{pmatrix} = \Sigma_{i=1}^{N} I\begin{pmatrix}y-(p+1-y)\\ y-(q+1-x)\end{pmatrix} \quad (8)$$

Here p,q are the sub image adjacent boundaries that are considered from an image.

Step-6: After the pixels are interchanged, the original image can be accessed by the new user based on their request.

Step-7: To access the image that is identified as duplicate, the image can be accessed by the use of hash value stored in the image header. The image is accessed as

$$I(x,y) = Mem\left(\frac{PiM(x,y) - HV(I_N(i,j)}{\text{count}(\ \forall(Mem(HV_N)\ )}\right) + Th \qquad (9)$$

Step-8: Display Decrypted Image D(I_N)
}

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.

4. RESULTS

In ANACONDA SPYDER, the proposed model is being implemented for decryption if compressed encrypted image is provided as input. Many safety checks to assess the efficiency of the technique indicated on photographs have been carried out. For one image, each pixel is highly correlated with its neighbouring pixels in horizontal, vertical or diagonal directions. Hash values are determined for the segments of each file that is newly uploaded and compared to a list of existing hash values [27]. If there is a match, the respective segment file is not stored, meaning that the segment file is duplicate. The proposed Image Decompression Model with Reversible Pixel Interchange Decryption model using Data Deduplication (IDRPID-DD) model is compared with the Chunk Based Deduplication Model (CDM) [24], Cipher Feedback based Electronic Code Book (CFB-ECB) model [25], Equal Modulus Decomposition (EMD) model [26] and Image Compression and Encryption Scheme based on Compressive Sensing (ICES-CS) [27] model and the results are represented.

A number of parameters including reversible pixel interchange time levels, decompression time levels, hash key generation time levels, decryption accuracy, decryption time levels, mean square error (MSE) [28] peak signal-to-noise ratio (PSNR) [29] and duplicate data identification time levels are being considered for the model proposed. A stable framework for the network image transmission is provided by the proposed model. The original image considered in this picture is represented in Figure 3.

Figure 3. Original image

The process of Denoising the image is performed and the noise is eliminated in the image before performing the compression technique. The Denoised image is shown in Figure 4.

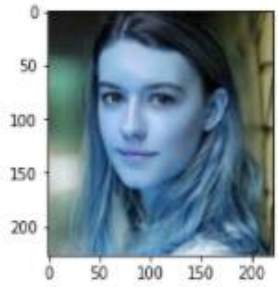

Figure 4. Denoised image

The proposed model performs reversible pixel interchange operation for restoring the pixels in the exact position. The pixels which are interchanged before encryption is restored using the reversible pixel interchange model and then decrypted. The proposed and traditional model time levels for reversible pixel interchange model is indicated in Figure 5.

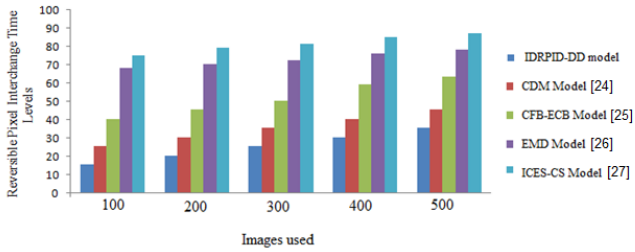

Figure 5. Reversible pixel interchange time levels

The image is converted into numerical data by extracting the pixel intensity values to perform the image processing operations. The Figure 6 represents the pixel intensity values of the image.

```
((227, 222, 3), array([[[ 25,  26,  24],
        [ 25,  26,  24],
        [ 25,  26,  24],
        ...,
        [163, 159, 101],
        [192, 188, 130],
        [174, 170, 111]],

       [[ 26,  27,  25],
        [ 26,  27,  25],
        [ 26,  27,  25],
        ...,
        [168, 164, 106],
        [193, 189, 131],
        [172, 168, 109]],

       [[ 26,  27,  25],
        [ 26,  27,  25],
        [ 26,  27,  25],
        ...,
        [167, 163, 105],
        [197, 193, 135],
        [182, 178, 119]],
```

Figure 6. Pixel intensity values

The grey level image is shown in Figure 7. The image will be converted into grey image to perform any image processing technique.

The image will be compressed at the sender side and then the data can be stored in cloud and can be utilized by receiver and then decompression is applied at the destination side. The image after applying the proposed compression technique is indicated in Figure 8.

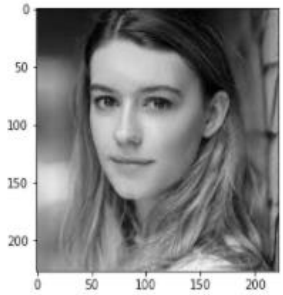

Figure 7. Grey image

Figure 8. Compressed image

After compression is applied, the image pixel interchanging model is applied so that the pixels positions are interchanged and the pixel interchanged image is shown in Figure 9.

Figure 9. Pixel interchanged image

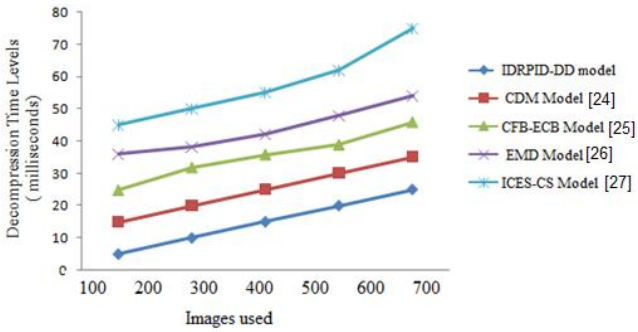

Figure 10. Decompression time levels

When data is compressed, files are transferred to a more compact alternative format than the original ones. The objective of this method is to reduce the memory space and transfer time available. The proposed considers the compressed image as input and then performs decompression on the image to extract the original image at the destination side. The proposed and traditional models decompression time levels are indicated in Figure 10.

The user has a private key and the hashing is applied over the image and the chipper block that pass through the hash checks and then the other user at the destination will decrypt the encrypted block with his public key and read the picture. The hash function is one-way function used in mapping any input size data to a fixed size called hash value for different purposes such as Image detection, duplicate image verification and image authentication. The proposed model hash key generation time levels are compared with the traditional model and the results are illustrated in Figure 11.

As information passes across the Internet, the access to unauthorised organisations or individuals needs to be monitored. This encrypts the data to reduce the loss of information and theft. Few popular encrypted objects include text, pictures, email, user data and directories. A prompt or window will be sent to the receiver for decryption to enter a password to access the encrypted data. The machine extracts and transforms the dysfunctions for decryption into words and images that are not only reader- and system-intensive. The proposed model decryption accuracy is compared with the traditional model and the results show that the proposed decryption accuracy is high. The decryption accuracy levels are represented in Figure 12.

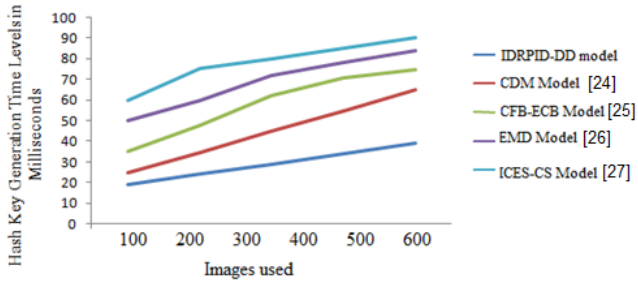

Figure 11. Hash key generation time levels

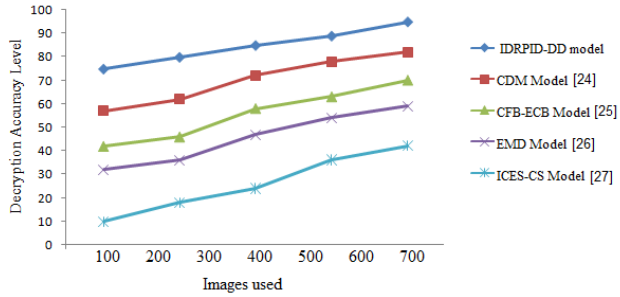

Figure 12. Decryption accuracy

The decryption time levels of the proposed and the existing models are indicated in Figure 13. The decryption time levels of the proposed model are less when compared to the traditional model. As the decryption time levels of the proposed model is less, the performance of the system will be improved.

The loss values range is shown in Figure 14. The training and testing loss values are calculated and represented clearly.

The huge growth of digital information in and its handling in storage services is a critical challenge currently, as it is loaded with a huge quantity of duplicate data in storage systems. In large-sized storage systems, replication is an effective technique. Duplication removes redundant data, enhances the use of storage and decreases storage costs. The duplicate data identification time levels are represented in

Figure 15. The duplicate data identification time levels of the proposed model are very less that represents that the proposed model performance levels are high than the existing models.

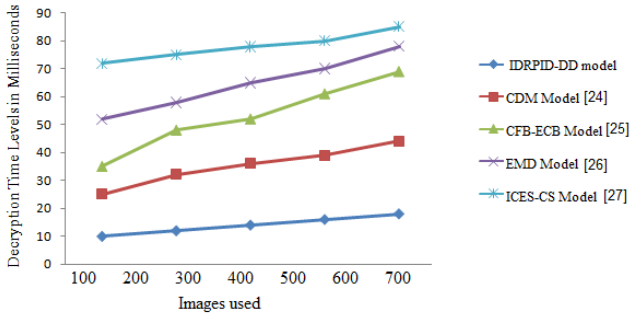

Figure 13. Decryption time levels

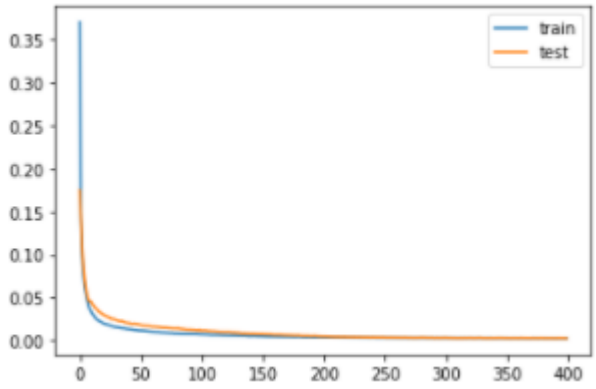

Figure 14. Loss values

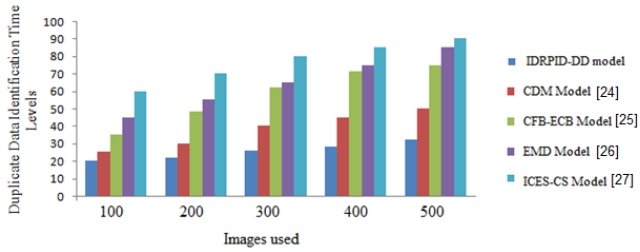

Figure 15. Duplicate data identification time levels

Table 1. Time for encryption for various picture sizes

Image size	Average Reversible Pixel Interchange Time (ms)	Average Decryption Time (ms)
256 x 256	4	5
512 x 512	9	15
1024 x 1024	21	63

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) (Table 1). 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 Figure 16.

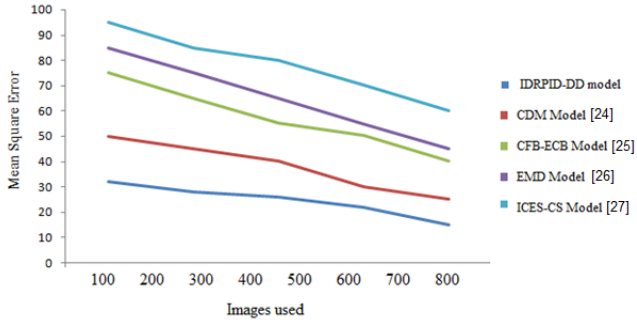

Figure 16. Mean square error

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

The Peak Signal-to-Noise Ratio (PSNR) representation of the proposed and the existing models are represented in Figure 17.

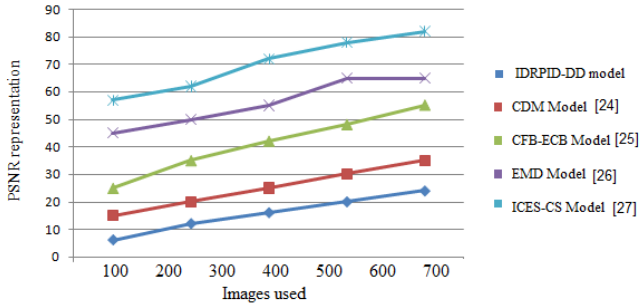

Figure 17. PSNR representation

5. CONCLUSION

Despite the many options available for storing data, including cloud data storage, the replication of data remains one of the main problems for users and organisations. It has been noted that there is a lot of replication of data for a single user or transaction arising from the use of multiple information sources. One of the efficient methods of data reductions is the deduplication of data. This technique ensures that each data is stored in a single copy. Data compression and encryption are becoming increasingly important as a means of increasing both productivity and security in communications. An efficient and secure structure for digital communication can be one that expresses two disparate but complementary actions on a single original file. Randomness is the adversary of compression, but encryption requires randomness in order to protect digital data. Compression and encryption are the two methods used here. It is hoped that the suggested approach may simultaneously compress and encrypt the random pixel interchange model. Subdivide each block into frequencies, execute pixel interchange, then encapsulate the resulting structure in a single block as part of the suggested method of picture compression and encryption. Every single block and sub block goes through the same procedure. Compression and encryption blocks swap pixels at random levels. Data that has been encrypted can be stored safely on the cloud. The data segments can be compared to existing stored data and therefore duplicate data is identified. In this article, an Image

Decompression Model with Reversible Pixel Interchange Decryption model using Data Deduplication is proposed. A compressed encrypted image with pixels interchanged is given as input and the proposed model performs the image decompression and performs reversible pixel interchange and then finally decrypts the data at the destination side and deduplication is performed to avoid memory wastage. A user who has the same picture copy can have the advantage of having access to the cipher text by transferring the evidence and removing his copy. If the attributes of a user match the access control setting of the owner, he may also download the images. Security review ensures confidentiality, data protection and comprehensiveness of this framework.

REFERENCES

[1] Wang, L., Wang, B., Song, W., Zhang, Z. (2019). A key-sharing based secure deduplication scheme in cloud storage. Information Sciences, 504: 48-60. https://doi.org/10.1016/j.ins.2019.07.058

[2] Li, C., Luo, G., Li, C. (2019). An image encryption scheme based on the three-dimensional chaotic logistic map. International of Journal Network Security, 21(1): 22-29. https://doi.org/10.6633/IJNS.201901 21(1).04

[3] Zahmoul, R., Ejbali, R., Zaied, M. (2017). Image encryption based on new Beta chaotic maps. Optics and Lasers in Engineering, 96: 39-49. https://doi.org/10.1016/j.optlaseng.2017.04.009

[4] Yavuz, E., Yazıcı, R., Kasapbaşı, M.C., Yamaç, E. (2016). A chaos-based image encryption algorithm with simple logical functions. Computers & Electrical Engineering, 54: 471-483. https://doi.org/10.1016/j.compeleceng.2015.11.008

[5] Zhang, Y. (2018). The unified image encryption algorithm based on chaos and cubic S-Box. Information Sciences, 450: 361-377. https://doi.org/10.1016/j.ins.2018.03.055

[6] Iqbal, N., Naqvi, R.A., Atif, M., Khan, M.A., Hanif, M., Abbas, S., Hussain, D. (2021). On the image encryption algorithm based on the chaotic system, DNA encoding, and castle. IEEE Access, 9: 118253-118270. https://doi.org/10.1109/ACCESS.2021.3106028

[7] Hamdi, M., Rhouma, R., Belghith, S. (2017). A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map. Signal Processing, 131: 514-526. https://doi.org/10.1016/j.sigpro.2016.09.011

[8] Setyaningsih, E., Harjoko, A. (2017). Survey of hybrid image compression techniques. International Journal of Electrical and Computer Engineering, 7(4): 2206. https://doi.org/10.11591/ijece.v7i4.pp2206-2214

[9] Setyaningsih, E., Wardoyo, R. (2017). Review of image compression and encryption techniques. International Journal of Advanced Computer Science and Applications, 8(2): 83-94.

[10] Zhang, Y. (2018). The unified image encryption algorithm based on chaos and cubic S-Box. Information Sciences, 450: 361-377. https://doi.org/10.1016/j.ins.2018.03.055

[11] Aqeel-ur-Rehman, X.L., Liao, X., Hahsmi, M.A.R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik-International Journal for Light and Electron Optics, 153: 117-134. https://doi.org/10.1016/j.ijleo.2017.09.099

[12] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons & Fractals, 95: 92-101. https://doi.org/10.1016/j.chaos.2016.12.018

[13] Zhang, Y. (2018). The unified image encryption algorithm based on chaos and cubic S-Box. Information Sciences, 450, 361-377. https://doi.org/10.1016/j.ins.2018.03.055

[14] Zhen, P., Zhao, G., Min, L., Jin, X. (2016). Chaos-based image encryption scheme combining DNA coding and entropy. Multimedia Tools and Applications, 75(11): 6303-6319. https://doi.org/10.1007/s11042-015-2573-x

[15] Qin, C., Zhou, Q., Cao, F., Dong, J., Zhang, X. (2018). Flexible lossy compression for selective encrypted image with image inpainting. IEEE Transactions on Circuits and Systems for Video Technology, 29(11): 3341-3355. https://doi.org/10.1109/TCSVT.2018.2878026

[16] Duan, X., Liu, J., Zhang, E. (2019). Efficient image encryption and compression based on a VAE generative model. Journal of Real-Time Image Processing, 16(3): 765-773. https://doi.org/10.1007/s11554-018-0826-4

[17] Kaur, M., Kumar, V. (2020). A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering, 27(1): 15-43. https://doi.org/10.1007/s11831-018-9298-8

[18] Kumari, M., Gupta, S. (2018). A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher. 3D Research, 9(1): 1-20. https://doi.org/10.1007/s13319-018-0162-2

[19] Kumari, M., Gupta, S., Malik, A. (2020). A superlative image encryption technique based on bit plane using key-based electronic code book. Multimedia Tools and Applications, 79(43): 33161-33191. https://doi.org/10.1007/s11042-020-09627-6

[20] Liu, X., Xiao, D., Xiang, Y. (2018). Quantum image encryption using intra and inter bit permutation based on logistic map. IEEE Access, 7: 6937-6946. https://doi.org/10.1109/ACCESS.2018.2889896

[21] Ye, G., Pan, C., Huang, X., Zhao, Z., He, J. (2018). A chaotic image encryption algorithm based on information entropy. International Journal of Bifurcation and Chaos, 28(1): 1850010. https://doi.org/10.1142/S0218127418500104

[22] Younes, M.A.B. (2019). A survey of the most current image encryption and decryption techniques. International Journal of Advanced Research in Computer Science, 10(1).

[23] Zhou, N., Chen, W., Yan, X., Wang, Y. (2018). Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Information Processing, 17(6): 1-24. https://doi.org/10.1007/s11128-018-1902-1

[24] Sun, W., Zhang, N., Lou, W., Hou, Y.T. (2018). Tapping the potential: Secure chunk-based deduplication of encrypted data for cloud backup. 2018 IEEE Conference on Communications and Network Security (CNS), pp. 1-9. https://doi.org/10.1109/CNS.2018.8433173

[25] Puteaux, P., Puech, W. (2021). CFB-Then-ECB mode-based image encryption for an efficient correction of noisy encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 31(9): 3338-3351. https://doi.org/10.1109/TCSVT.2020.3039112

[26] Luan, G., Li, A., Chen, Z., Huang, C. (2020). Asymmetric optical image encryption with silhouette removal using interference and equal modulus decomposition. IEEE Photonics Journal, 12(2): 1-8. https://doi.org/10.1109/JPHOT.2020.2963921
[27] Zhang, M., Tong, X., Liu, J., Wang, Z., Liu, J., Liu, J., Ma, J. (2020). Image compression and encryption scheme based on compressive sensing and Fourier transform. IEEE Access, 8: 40838-40849. https://doi.org/10.1109/ACCESS.2020.2976798
[28] Xia, W., Jiang, H., Feng, D., Douglis, F., Shilane, P., Hua, Y., Zhou, Y. (2016). A comprehensive study of the past, present, and future of data deduplication. Proceedings of the IEEE, 104(9): 1681-1710. https://doi.org/10.1109/JPROC.2016.2571298
[29] Kambo, H., Sinha, B. (2017). Secure data deduplication mechanism based on Rabin CDC and MD5 in cloud computing environment. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 400-404. https://doi.org/10.1109/RTEICT.2017.8256626