DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

RCAE_BFV: Retrieve Encrypted Images Using Convolution AutoEncoder and BFV

Emad M. Alsaedi[1], Alaa kadhim Farhan[2]
[1,2]*Computer Sciences Department, University of Technology, Baghdad, Iraq*
[1]*cs.19.71@grad.uotechnology.edu.iq*, [2]*Alaa.K.Farhan@uotechnology.edu.iq*

Abstract— *Content-Based Image Retrieval (CBIR) is an actual application in computer vision, which retrieves similar images from a database. Deep Learning (DL) is essential in many applications, including image retrieval applications. However, encryption techniques are used to protect data privacy because these data are vulnerable to being viewed by unauthorized parties while being transmitted over unsecured channels.*

This paper includes two parts for images retrieval. In the first part, features of all images of a Canadian Institute for Advanced Research CIFAR-10 dataset were extracted and stored on the Server-side. In the second part, the Brakerski/Fan-Vercauteren (BFV) homomorphic encryption scheme method for encrypting an image sent by the client-side. First, their decryption and image features are extracted depending on the trainer model when they arrive on the server-side. Then an extracted features are compared with stored features using the Cosine Distance method, and then the server encrypts the retrieved images and sends them to the client-side. Deep-learning results on plain images were 97% for classification and 96.7% for retriever images. At the same time, The National Institute of Standards and Technology (NIST) test was used to check the security of BFV when applied to CIFAR-10 dataset.

Index Terms— *BFV, Convolution Autoencoder, Content-based image retrieval, Homomorphic encryption.*

I. INTRODUCTION

Content-Based Image Retrieval is a technique that improves the precision of the image search process and thus the image retrieval accuracy. Many authors worked on image processing concepts based on CBIR systems, which use color, texture, direction, orientation, grayscale, and shape techniques. Processing this yields a feature vector, which completes the comparison process. The CBIR method has been used for registration, face detection, etc., in search engines and patents. The CBIR method, which is meant to help prevent data breaches, could be used for security purposes. These days, the transmission of data without leakage is an important topic. Many methods have been proposed for data encryption. These methods can perform both the encryption and decryption processes of the images[1][2]. There has been an increase in worry about the security of digital images delivered through open or stored networks due to the dynamic expansion of the multimedia and communication business. Because of the unauthorized use of digital images, it is vital to secure images. Some cryptographic systems, such as Advanced Encryption Standard (AES) or International Data Encryption Standard (IDES), can be used to protect data[3]. Using Fully Homomorphic Encryption (FHE) , the model can perform an unbounded computation over ciphertext and decrypt it into plain text . The Eq.(1) shows how a function *f*() takes plaintext numbers (such as addition or multiplication) and produces ciphertext. [4].

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

$$f\big(E(m)\big) = E\big(f(m)\dot{\big)} \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Armknecht and Sadeghi developed an algebraically homomorphic approach to cryptography in 2008 [5]. While Gentry extended foundational work on fully homomorphic schemes in 2009 [6]. The same year Gentry modified fully homomorphic encryption utilizing ideal lattices [7]. Van Dijk et al. developed completely homomorphic encryption over integers in 2010 [8]. Gentry et al. (2013) also developed homomorphic encryption based on error learning [9]. *Fig. 1* illustrates the approach of completely homomorphic cryptosystems.

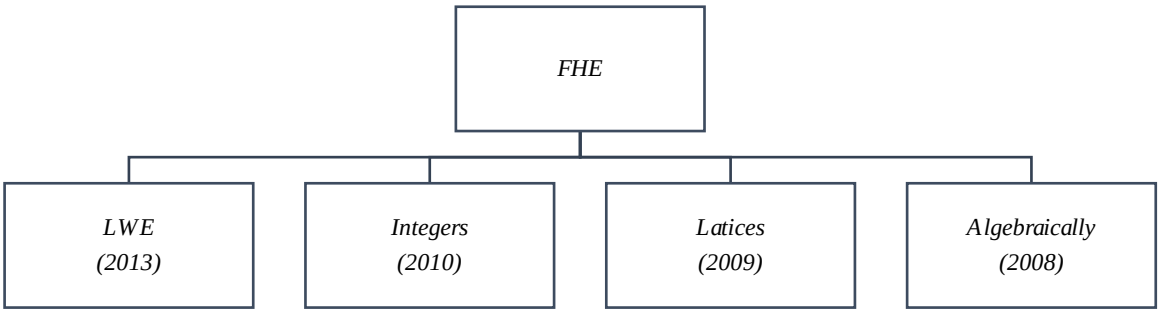

FIG. 1. APPROACH OF THE FHE.

Schemes that are completely homomorphic BFV are defined over the cyclotomic polynomial of degree m. The ring is used as the plaintext space for the BFV system. A distinguishing feature of the BFV system and its derivatives is that they permit Single Instruction, Multiple Data (SIMD) parallel processing[10].

The learning algorithms in use today are founded on predefined, hand-designed characteristics: deep learning, one of the most efficient machine learning approaches. To effectively use a deep learning model, it must first be trained to increase its accuracy. Afterward, the model may be used for various applications, such as classification or prediction. The use of deep learning has expanded dramatically in recent years, especially in big data analytics and the detection of patterns, speech recognition, and computer vision. Using a more advanced cloud architecture and a collaborative approach raises privacy issues, especially deep learning. The privacy concerns that are now developing are associated with sensitive input data used in training or inference and with sharing models that have been trained. Using a powerful server or cloud located elsewhere will increase the training algorithm's efficiency. [11]. The difficulty with these environments is that the end-users and the server both have privacy concerns. Under some circumstances, an adversary who knows everything about it might exploit the training process, leading to privacy issues and deflecting attention from data privacy to model privacy. [12].

This paper includes the following contributions: Using deep learning techniques to propose an effective solution for image retrieval. FHE-BFV encryption is applied to the transmitted images to assure their security. Training Convolution AutoEncoder (CAE) on augmented images will help it improve its classification accuracy. It utilizes the Random Forest algorithm to identify the most accurate features that are less time-consuming to retrieve.

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

II. RELATED WORKS

A large amount of research has been published in the fields of CBIR and homomorphic encryption.

Mohammad et al.,[13] CAE deep learning technology propose a CBIR system for Breast UltraSound (BUS) images. First, a CAE is explicitly created to extract a vector of 32 latent features for representing the BUS image. Second, a similarity measure identifies and retrieves the most relevant BUS images from reference BUS images relevant to the query image database based on latent features.

Fathala et al.,[4] This paper are essentially dependent on two procedures to retrieval techniques. First, extract image features with the histogram, then use statistical features (mean, standard deviation). In this instance, the T-test is used to examine the relationship between many different images.

Maria et al.,[14] The deep Convolution Neural Network (CNN) model was utilized in this paper to create feature representations from convolutional layer activations via max-pooling to image retrieval processing. Three fundamental model retraining methodologies are proposed. If no information other than the dataset itself is available, the Fully Unsupervised Retraining, if the labels of the training dataset are accessible, and the Relevance Feedback based Retraining, if user feedback is provided.

In their paper for image retrieval, Kuo et al. [15] introduced deep convolutional neural networks. It uses DL to train the weights of a Neural Network (NN), resulting in high-level image feature extraction.

Hsin et al. [16] proposed CNN as an aggregate of ensemble models for image retrieval. This image classifier combines AlexNet and Network in Network (NIN), particularly effective deep learning networks, to achieve image feature extraction. It computes weighted average feature vectors for image retrieval.

Umer et al. [17] developed an efficient content-based image retrieval CBIR system capable of retrieving correct images semantically. They proposed a hybrid features descriptor consisting of color and texture features for this purpose.

n this article, Gautam et al. [18] initially extracted texture features with Dual-Tree Complex Wavelet Transform (DTCWT) to solve the problem of repetitive Complex Wavelet Transform CWT. Then, to improve computation and efficiency, extract color features from RGB and HSV color spaces using Dominant Color Descriptors (DCD). There are 1000 images in the experimental dataset that has been used. The Weighted Euclidean Distance is used to compute the equal dimension (WED). To improve the system's performance, utilize ACO for the best results and SVM to categorize data.

Clet et al. [19] comprehensively covered the three most common homomorphic cryptosystems are Brakerski/Fan- Vercauteren (BFV), Cheon–Kim–Kim–Song (CKKS), and : Fast Fully Homomorphic Encryption (TFHE). Concerning the training phase of feed-forward neural networks completed on the Modified National Institute of Standards and Technology database MNIST dataset.

Jung and et al. [20] devised a method to refresh low-level ciphertexts based on Gentry's bootstrapping procedure, extending the leveled homomorphic encryption strategy for approximate arithmetic. In addition, they provide an efficient evaluation technique and use a scaled sine function to approximate the modular reduction process.

Wei et al. [21] proposed a secure computing technique for the Internet of Things (IoT). In this study, An efficient BFV-type homomorphic encryption scheme has been used. This

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

system aims to reduce the amount of storage space required for switch keys and the amount of time required for ciphertext assessment.

III. MATERIALS

In the CIFAR-10 dataset, various images are used to train machine learning algorithms and computer vision algorithms. So this dataset is becoming increasingly popular among researchers conducting machine learning research. Each image in the CIFAR-10 dataset is 32x32 pixels in size and is saved in the Portable Network Graphics (PNG) format. The images are divided into ten categories, and the dataset has 60,000 images in total. Classifications include things like an airplane, a car, a bird, a cat, a deer, a dog, a frog, a horse, a ship, and a truck.

IV. DEEP LEARNING

Deep learning has demonstrated significant betterment in visual processing. Image retrieval is the process of retrieving visually similar images from a store for a query image. The feature similarity is used to rate the images. Many designed elements have been developed in recent years to depict the images. one of the most important deep learning models for learning the latent space is autoencoders[22]. Using Convolutional Neural Networks for image analysis has been demonstrated to be effective . The neurons, weights, and biases of a CNN are similar to those of a feed-forward neural network. Dot products of neighboring weights and neuron inputs are utilized as input to a rectification unit in each neuron, which is then employed as a bias (ReLu). A convolution layer, a max-pooling layer, and a fully-connected layer are all included in a single layer CNN[23]. The CNN nodes are driven by their activation functions that may vary between a node and another in the same model. Some of those activation functions are tanh, sigmoid, and ReLU. The Adam function may be used as one of the optimizing for model training[24].

V. HOMOMORPHIC ENCRYPTION (HE)

Various tools are employed to protect privacy, such as differential privacy techniques and homomorphic encryption. HE is a type of encryption that allows various kinds of calculations to be performed on ciphertexts to produce an encrypted output. HE is divided into three categories [25].

***A. Partially Homomorphic Encryption (PHE)*:** This provides only one encrypted data process, either addition or multiplication.

B. Somewhat Homomorphic Encryption (SWHE): This provides more than one process, such as multiplication and addition, but the number of operations is limited.

***C. Fully Homomorphic Encryption FHE*:** This provides multiple multiplication and addition processes without restricting the number of functions.

HE schemes include four stages. [26]***:***

1. **The Key Generation (KeyGen)**: In this stage, security parameters are generated. In an asymmetric type, a single key is generated, while a pair of secret and public keys are generated in an asymmetric type.

2. The Encryption Algorithm (Enc): This stage encrypts the plaintext inputs message, m ϵ M, with the encryption key. The ciphertext is generated by c = Enc(m), where c ∈ C, C is the ciphertext space.

3. The Decryption Algorithm (Dec): In this stage, the original message is recovered by decrypting ciphertext c using the decryption key ((c) = m).

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

4. **The Evaluation Algorithm (Eval):** This stage performs the evaluations of the ciphertexts $(c1,\ c2)$,$(c1,\ c2)$ = $Eval\ \{(m1,\ m2)\}$, without revealing the messages $(m1,\ m2)$.

VI. BFV FULL HOMOMORPHIC ENCRYPTION

The plaintext space is $\mathbb{Z}_p[X]/(X^N+1)$, where the plaintext modulus p is an integer, and the polynomial degree N is a power of 2 . Let q be the ciphertext modulus. The cryptosystem is composed of the following algorithms[19] :

- Secret Key generation: The secret key s is a sample from a random distribution over a subspace of $\mathbb{Z}_p[X]/(X^N+1)$.
- Public key generation: Given an element a sampled from a uniform distribution over $\mathbb{Z}_q[X]/(X^N+1)$ and an element ***e*** sampled from an error distribution (usually Gaussian) over $\mathbb{Z}_q[X]/(X^N+1)$, the public key is computed
- Encryption: Let $\mu \in \mathbb{Z}_p[X]/(X^N+1)$ be a message. *Let u, e1*, and *e2* be small errors. Then encrypt the message as $c = \left([p_0.u + e1 + \Delta.\mu]_q, [p_1.u + e2]_q\right) = (c0, c1)$
- – Decryption: can then retrieve the messages thanks to the following function $[\left\lceil \frac{p.[c0+c1.s]q}{q} \right\rfloor]_q$.The noise must be lower than Δ/2 for this operation

VII. CONVOLUTIONAL AUTOENCODER

Autoencoder is a form of deep neural network use to learn efficient codings from unsupervised learning. By trying to recreate the input from the encoding, the encoding is checked and enhanced. By training the network to reject inconsequential input ("noise"), the autoencoder learns a representation (encoding) for a collection of data, generally for dimensionality reduction. The CAE is an autoencoder used to represent the input image x using a reduced form known as vector z . This procedure is carried out in conventional autoencoders by an encoding function, a decoding function, and a loss function. The encoder, defined by f(x), transforms the original image, x, into the compressed representation, z, with z having a lower dimensionality than x. Meanwhile, the decoder reconstructs image x, analyzes the determining, z, to recreate a clone of the image. As a result, the reconstructed image can be stated as x = g(f(x)[13].

VIII. PROPOSED SYSTEM

The proposed RCAE_BFV is consists of two major phases, as shown in *Fig. 2*. the offline phase is implemented on the server-side, and the online phase is implemented on both the server and the client. Each CIFAR's images were evaluated offline using the CAE to extract latent features used in the next phase to retrieve images. The online phase consists of eight steps on the server side and four steps on the client-side. On the server-side, the initial step is to generate the keys. Second, route them to the client's side. The third step is to receive the encrypted image. The fourth step is to decrypt the encrypted image. Fifth, use the CAE model to extract latent features from the decrypted image, and sixth, deliver the decrypted image.

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

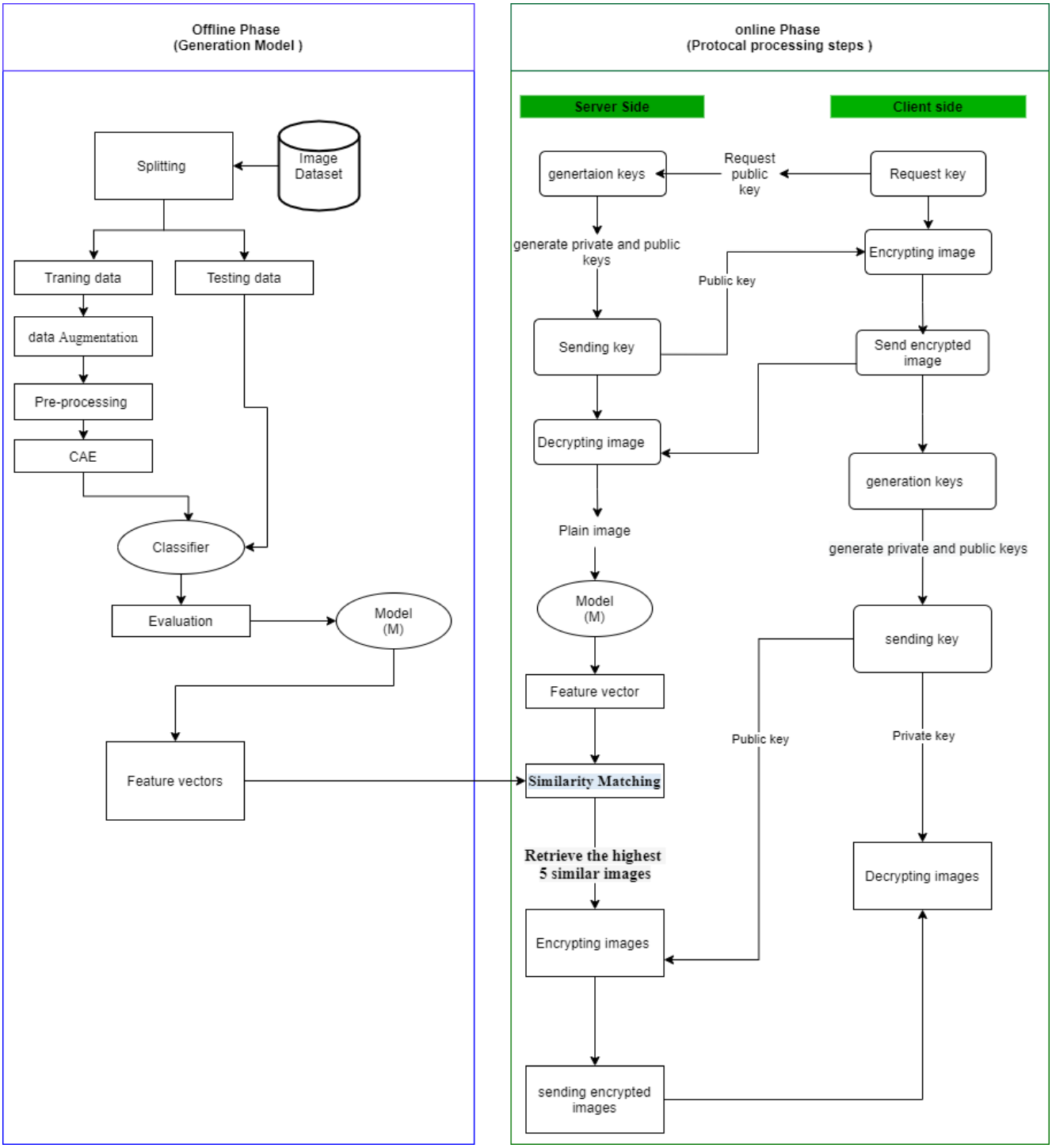

FIG. 2. RCAE_BFV PROTOCOL WHICH CONSISTS OF OFFLINE AND ONLINE PHASES.

A. Offline phase

This part has two major stages: the first contains a trained model (M), and the second uses the trained model to extract the features for each image in the training dataset. The image datasets used in this article include CIFAR-10 (Canadian Institute for Advanced Research) is contains 60,000 images in the PNG format with a size of 32x32 colors. This dataset is divided into two parts, the training dataset, and the test dataset. The training dataset consists of 50,000 images for training the network, accounting for 80% of the total

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

dataset. On the other hand, the test data set comprises 10,000 images for testing the network and accounts for 20% of the entire dataset. Ten proper augmentations are employed in the proposal system: rotating, horizontal shifting, vertical shifting, and flipping. The rotation process is applied to the original training images at an angle of 15 degrees, which generates a new 50,000 images using the Bilinear interpolation method. An image can be shifted horizontally and retain the exact dimensions without distorting it by using horizontal shift augmentation. The process of shifting all the pixels vertically while maintaining the image dimensions is referred to as vertical shift augmentation. The neighborhood of each pixel is thresholded, and a result is a binary number with LBP. Other augmentation methods, which use Gaussian blurring to generate new images, are currently under development.

Furthermore, two noise-generating techniques are employed. These are Gaussian and Salt-and-pepper noise. A total of 450,000 training images are produced as a result.

Fig. 3 illustrates the network architecture of CAE.

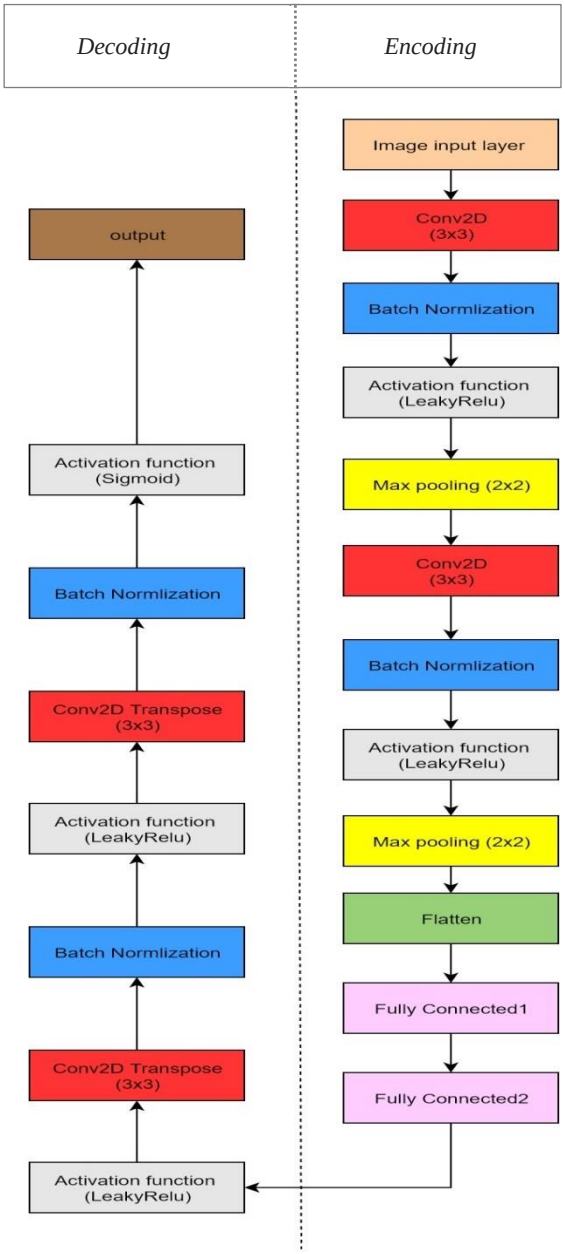

FIG. 3. THE PROPOSED CAE ARCHITECTURE AS DRAWN BY NETRON SOFTWARE.

Received 27/September/2021; Accepted 9/December/2021

ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

For the encoder network, use two convolutional layers followed by a fully-connected layer. The decoder network mirrors this architecture by using a fully-connected layer followed by three convolution transpose layers. The CAE consists of two classifiers: one that is learned in an unsupervised learning environment, and the other uses a Fully Connected Network (FCN) classifier. As a substitute for traditional CAE, CNN-based CAE is employed. For the FCN classifier, researchers then need two fully connected (FC) layers. For learning the features, CAE is utilized using RGB picture values as input data. The following is a definition of the new feature learning: Amount of information provided To begin, all images of trains were sent over the CAE network. A network that converts input data into an encoded form as output is called an encoder. The decoder's output size is configured to be less than the input size. Because the encoder network's output serves as the latest features, the network's output size is configured to match the latent features 'size. The latent features of the CAE model are represented by the mean and variant values (z) of the probability distribution q(z/x), respectively. Its latent features describe X's features.

B. Online processing phase

This phase begins when the client requests the public key from the server to encrypt the image and later sends the encrypted image to the server. In this phase using BFV as the FHE algorithm, the client initially takes a message (M) and convert it to cipher vectors ([⟨ct1,pk⟩]%q,[⟨ct2,pk⟩]%q), where ct1 and ct2 are ciphertexts represented in polynomial form, pk represents the public key, and q refers to the ciphertext modulus.

Generating keys step (server-side, client-side): Both public (pk) and private keys (SK) are generated on the server-side and the client, and each side uses its keys to accomplish the encryption and decryption operations.:

Encrypting image (server-side, client-side): After receiving the public key from the client, the client performs the image encryption procedures. It resizes the image to scale 32x32 using the bilinear method, resizes all images, then reads the image pixel by pixel and encodes each using BFV encoding. In this step, every pixel in the image is converted into a polynomial with degree 8. Also, the server-side encrypts the retrieved images in the same manner but with the client's public key.

Decrypting image (server-side, client-side): The encrypted image was created on the client-side and depended on the public key sent by the server. This image is sent to the server to retrieve the top five similar images to this image. This process decrypts the image with the private key generated on the server-side. The output of the decryption process is in a polynomial form, so decoding of the output is used to retrieve the actual values of the pixels. The client also utilizes the private key to open images received from the server in the same way that the server does.

Similarity matching (server-side only): This step of the image retrieval process, using the model (M), extracts the features of the sent image based on the flatten layer. The Hamming distance approach is used to determine the similarity of the five most similar images to the sent image using the features extracted and the feature vectors stored in the training phase.

IX. RESULT

There are many results from this proposed model illustrated as follows:

A. Augmentation data result

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

Fig. 4 shows an example of the four augmentations used, the rotating, horizontal shifting, vertical shifting, and flipping, and Table I shows the dataset size after applying the augmentation data.

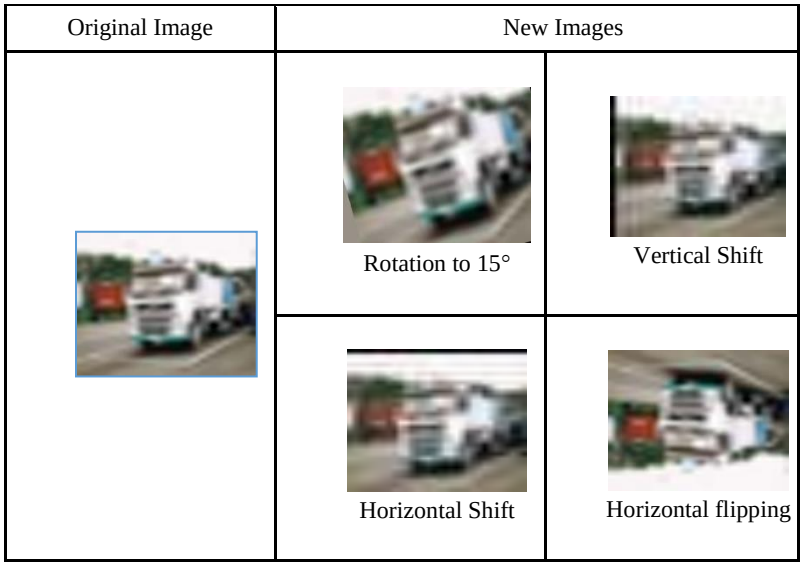

FIG. 4. RESULT OF THE AUGMENTATION PROCESS.

TABLE I. DATASET SIZE AFTER APPLIED DATA AUGMENTATION

Dataset Type	No. of images
Original training dataset	50,000
Rotation dataset	50,000
Horizontal shift dataset	50,000
Vertical shift dataset	50,000
Gaussian blurring	50,000
Horizontal flipping dataset	50,000
Local Binary Pattern	50,000
Gaussian noise	5,0000
Salt-and-pepper noise	50,000
Total	450,000

B. Training Results

The model has been trained on 450,000 images (450,000 R, 450,000 G, 450,000 B) training images using optimization method RMSprop with an initial learning rate of 0.001.

The dataset goes through 200 epochs to enhance the images. In every epoch, the weights are changed to get the image closer to the desired image. Table II illustrates the model accuracy and loss with the corresponding hyperparameters through the training stage.

Received 27/September/2021; Accepted 9/December/2021

ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

TABLE II. TRAINING RESULTS

Iteration	**Batch size**	**Learning rate**		**Loss function**	**Optimizer**	**Epochs**	**ETA**		**VAL-Loss**	**VAL-Accuracy**	**Loss**	Accuracy
		Initial value	**Last value**									
781	64	0.001	0.0004	Categorical cross-entropy	RMS prop	200	875s		0.4714	0.97	0.3276	0.97

C. Testing Results

The 10,000 testing images, representing 20% of the CIFAR-10 dataset, have been input into the model architecture and gone through all its layers. Using the saved parameters, including the weights that the network reached and multiplying them by those weights, the testing images classify into ten classes. Table III illustrates the results of testing accuracy, the time estimate for testing and the loss value.

TABLE III. PERFORMANCE OF TESTING

ETA	**LOSS**	**ACCURACY**
58S 4MS	0.410	97%

D. NIST Tests Results

This part presents the result NIST for the BFV algorithms on the CIFAR dataset. In this test, the results converted from the cipher data, which is in the polynomial format, to binary, and then the NIST measurements were tested. Table IV and *Fig. 5* illustrates the results of this test.

TABLE IV. NIST TEST RESULTS OF THE BFV ALGORITHM

Test	**BFV Algorithm**	**Pass**
Run	0.654788	True
serial	0.276586	True
random excursion variant	0.564785	True
random excursion	0.897657	True
non-overlapping template matching	0.456378	True
Frequency Monbiot	0.674689	True
Maurer's universal statistical	0.984753	True
the longest run of ones in a block	0.786403	True
Linear complexity	0.783549	True

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

Frequency test within a Block	0.987364	True
Discrete Fourier transform	0.637928	True
Cumulative sums	0.047382	True

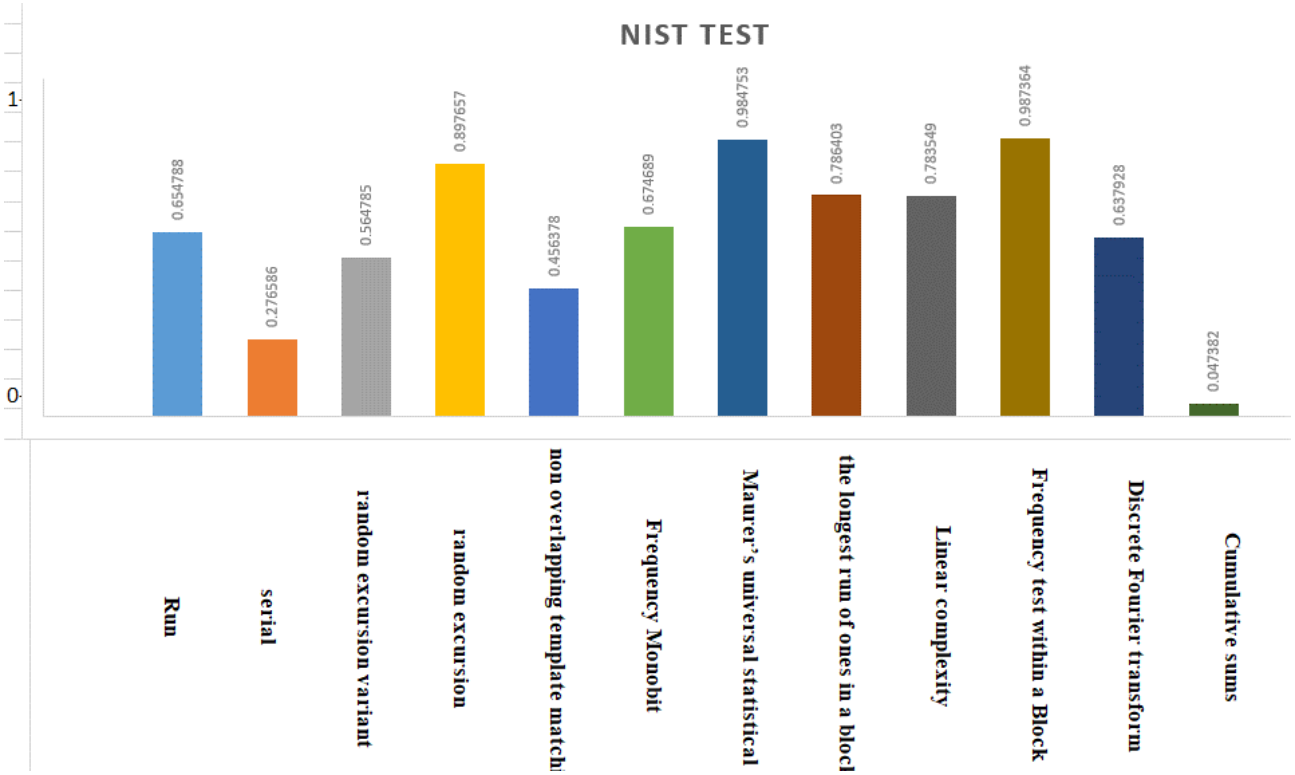

FIG. 5. NIST TEST RESULTS OF THE BFV ALGORITHM.

E. Timing test

Table V displays the time results for each encryption algorithm and deep learning method and the image retrieval time. All trials were performed on a computer with a dual-core processor, a clock speed of 2.7 GHz, and a memory capacity of 4 GB with pre-installed Windows 7.

TABLE V. TIME RESULTS

BFV		**CAE model (seconds)**		**Retrieve each image (seconds)**
Encryption each image (seconds)	Decryption each image (seconds)	Traini ng	testing	
23	21	46800	3670	0.06

F. Comparison with Previous Studies

Several methods have been proposed to enhance the retrieved images. Table VI, *Fig. 6*, and Table VII, *Fig. 7* illustrate the results of these methods.

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

TABLE VI. IMAGE CLASSIFICATION ACCURACY ON CIFAR-10

	Image classification accuracy
Kua et al. [21]	96.9
Hsin et al. [22]	90.19
RCAE_BFV	97

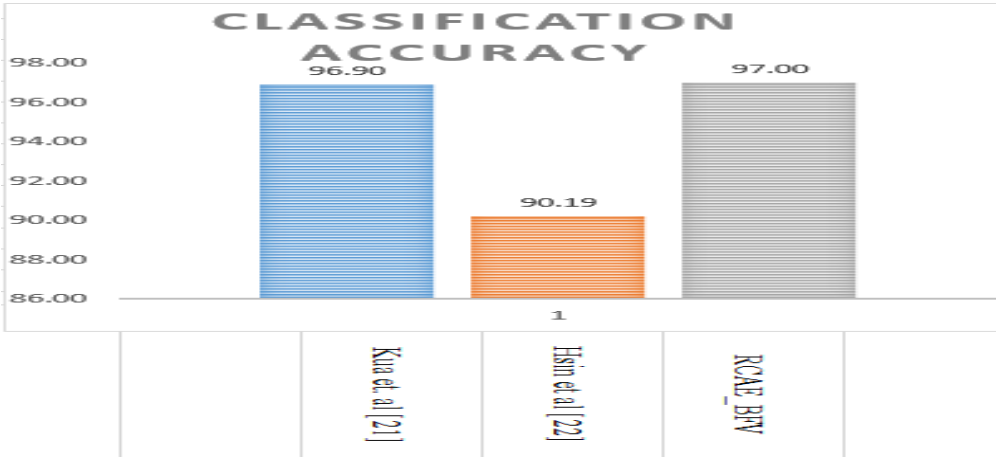

FIG. 6. IMAGE CLASSIFICATION ACCURACY ON CIFAR-10.

Table VII. shows the retrieval performance for CIFAR-10 datasets in mean average precision for different research projects.

TABLE VII. IMAGE RETRIEVAL MAP ON CIFAR-10

	MAP
Kua t al [21]	0.707
Hsin et al. [22]	0.867
Umer et al. [23]	0.913
RCAE_BFV	0.9`67

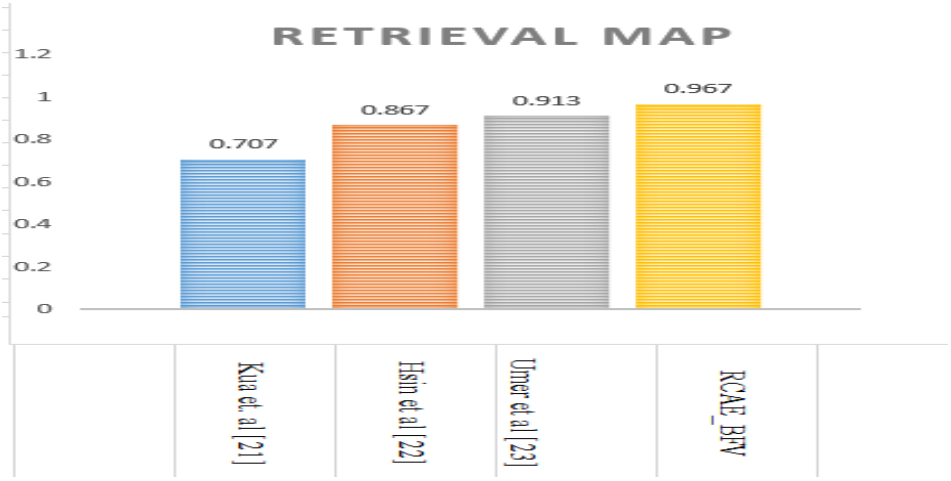

FIG. 7. IMAGE RETRIEVAL MAP ON CIFAR-10.

Received 27/September/2021; Accepted 9/December/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

X. DISCUSSION

Related work studied in this research included results less than this research. The presented results showed that the CAE suggested in this research was distinguished from other research with higher results in the classification and retrieval process. This research noted that the flatting layer provided features used by retrieving similar images because this layer contains properties that depend on trained weights in the training phase. The Random forest method has been used to choose the best features that give better results in terms of accuracy and time. In addition, the proposed data augmented method led to an increase in dataset samples used to overcome the problems of overfitting and increase the accuracy of training and noticed through previous research that the security of the data sent through the network is not taken. Most of the applications that need image retrieval are applications that need to maintain the privacy of the data of the sending person, so proposed a protocol that maintains data privacy.

XI. CONCLUSIONS

This paper has presented an effective content-based image retrieval CBIR system capable of semantically retrieving the correct images with high retrieval performance. For this purpose, researchers proposed a method for image retrieval based on CAE developed by taking advantage of the flatten layer, which extracts 4096 image features stored in one feature vector. Next, researchers applied the random forest algorithm after this layer as features selection to produce 1024 features that contribute increased accuracy compared to the previous research. The researchers developed the secure to preserve the data communicated through an insecure connection between the client and the server using BFV to provide the highest security. It also overcomes the overfitting issue and improves the model's accuracy by increasing the number of training images to use eight different augmentation methods. Finally, noted that the BFV approach is slow and requires more cipher image space, yet it is a powerful encryption method.

REFERENCES

[1] M. K. Chigateri and S. Sonoli, "CBIR algorithm development using RGB histogram-based block contour method to improve the retrieval performance," *Mater. Today Proc.*, no. xxxx, 2021, doi: 10.1016/j.matpr.2021.03.198.

[2] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, pp. 1–14, 2019, doi: 10.3390/e21100958.

[3] A. S. Hamad and A. K. Farhan, "Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme," *Eng. Technol. J.*, vol. 38, no. 3B, pp. 98–103, 2020, doi: 10.30684/etj.v38i3b.433.

[4] F. Ali and A. H. Mohammed, "Content Based Image Retrieval (CBIR) by statistical methods," *Baghdad Sci. J.*, vol. 17, pp. 694–700, 2020, doi: 10.21123/bsj.2020.17.2(SI).0694.

[5] F. Armknecht and A. Sadeghi, "A New Approach for Algebraically Homomorphic Encryption.," *IACR Cryptol. ePrint Arch.*, 2008, [Online]. Available: http://eprint.iacr.org/2008/422.pdf?origin=publication_detail.

[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," 2009.

[7] C. S. Gu, "Fully homomorphic encryption from approximate ideal lattices," *Ruan Jian Xue Bao/Journal Softw.*, vol. 26, no. 10, pp. 2696–2719, 2015, doi: 10.13328/j.cnki.jos.004808.

[8] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," pp. 24–43, 2010.

[9] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8042 LNCS, no. PART 1, pp. 75–92, 2013, doi: 10.1007/978-3-642-40041-4_5.

Received 27/September/2021; Accepted 9/December/2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.3.5

[10] H. Zong, H. Huang, and S. Wang, "Secure Outsourced Computation of Matrix Determinant Based on Fully Homomorphic Encryption," *IEEE Access*, vol. 9, pp. 22651–22661, 2021, doi: 10.1109/ACCESS.2021.3056476.

[11] A. Boulemtafes *et al.*, "A review of privacy-preserving techniques for deep learning To cite this version : HAL Id : hal-02921443 A Review of Privacy-Preserving Techniques for Deep Learning," 2020.

[12] D. Zhang, X. Chen, D. Wang, and J. Shi, "A survey on collaborative deep learning and privacy-preserving," *Proc. - 2018 IEEE 3rd Int. Conf. Data Sci. Cyberspace, DSC 2018*, pp. 652–658, 2018, doi: 10.1109/DSC.2018.00104.

[13] M. I. Daoud, A. Saleh, I. Hababeh, and R. Alazrai, "Content-based Image Retrieval for Breast Ultrasound Images using Convolutional Autoencoders: A Feasibility Study," in *BioSMART 2019 - Proceedings: 3rd International Conference on Bio-Engineering for Smart Technologies,IEEE*, 2019, pp. 1–4, doi: 10.1109/BIOSMART.2019.8734190.

[14] M. Tzelepi and A. Tefas, "Deep convolutional learning for Content Based Image Retrieval," *Neurocomputing*, vol. 275, pp. 2467–2478, 2018, doi: 10.1016/j.neucom.2017.11.022.

[15] C. H. Kuo, Y. H. Chou, and P. C. Chang, "Using deep convolutional neural networks for image retrieval," in *IS and T International Symposium on Electronic Imaging Science and Technology*, 2016, pp. 1–6, doi: 10.2352/ISSN.2470-1173.2016.2.VIPC-231.

[16] H. K. Huang, C. F. Chiu, C. H. Kuo, Y. C. Wu, N. N. Y. Chu, and P. C. Chang, "Mixture of deep CNN-based ensemble model for image retrieval," *2016 IEEE 5th Glob. Conf. Consum. Electron. GCCE 2016*, no. 2, pp. 5–6, 2016, doi: 10.1109/GCCE.2016.7800375.

[17] U. A. Khan, A. Javed, and R. Ashraf, "An effective hybrid framework for content based image retrieval (CBIR)," *Multimed. Tools Appl.*, vol. 80, no. 17, pp. 26911–26937, 2021, doi: 10.1007/s11042-021-10530-x.

[18] A. Gautam and R. Bhatia, "A Novel Method for CBIR Using ACO-SVM with DTCWT and Color Features," *Mater. Today Proc.*, vol. 5, no. 1, pp. 1439–1446, 2018, doi: 10.1016/j.matpr.2017.11.231.

[19] P.-E. Clet, O. Stan, and M. Zuber, *BFV, CKKS, TFHE: Which One is the Best for a Secure Neural Network Evaluation in the Cloud?* Springer International Publishing, 2021.

[20] J. H. Cheon, K. Han, A. Kim, M. Kim, and Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers," in *International Conference on the Theory and Application of Cryptology and Information Security,Springer*, 2017, pp. 409–437, doi: 10.1007/978-3-319-78381-9_14.

[21] W. Yuan and H. Gao, "An efficient BGV-type encryption scheme for IoT systems," *Appl. Sci.*, vol. 10, no. 17, 2020, doi: 10.3390/APP10175732.

[22] S. R. Singh, S. R. Dubey, S. MS, S. Ventrapragada, and S. S. Dasharatha, "Joint Triplet Autoencoder for Histopathological Colon Cancer Nuclei Retrieval," 2021, [Online]. Available: http://arxiv.org/abs/2105.10262.

[23] A. J. Abidalkareem, M. A. Abd, A. K. Ibrahim, H. Zhuang, A. S. Altaher, and A. Muhamed Ali, "Diabetic Retinopathy (DR) Severity Level Classification Using Multimodel Convolutional Neural Networks," *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, vol. 2020-July, pp. 1404–1407, 2020, doi: 10.1109/EMBC44109.2020.9175606.

[24] A. Altaher, Z. Salekshahrezaee, A. A. Zadeh, A. Salem, and A. Altaher, "Using Multi-inception CNN for Face Emotion Recognition Ali Salem Altaher," *Bioeng. Res.*, vol. 3, no. June, pp. 1–12, 2021, doi: 10.22034/jbr.2021.262544.1037.

[25] M. A. Will and R. K. L. Ko, *A guide to homomorphic encryption*. Elsevier Inc., 2015.

[26] R. Shrestha and S. Kim, *Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities*, 1st ed., vol. 115. Elsevier Inc., 2019.

Received 27/September/2021; Accepted 9/December/2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*