# *Z*-Score-Based Secure Biomedical Model for Effective Skin Lesion Segmentation Over eHealth Cloud

AMITESH SINGH RAJPUT, Birla Institute of Technology and Science (BITS) Pilani, India
VISHESH KUMAR TANWAR and BALASUBRAMANIAN RAMAN, Indian Institute of Technology Roorkee, India

This study aims to process the private medical data over eHealth cloud platform. The current pandemic situation, caused by Covid19 has made us to realize the importance of automatic remotely operated independent services, such as cloud. However, the cloud servers are developed and maintained by third parties, and may access user's data for certain benefits. Considering these problems, we propose a specialized method such that the patient's rights and changes in medical treatment can be preserved. The problem arising due to Melanoma skin cancer is carefully considered and a privacy-preserving cloud-based approach is proposed to achieve effective skin lesion segmentation. The work is accomplished by the development of a *Z*-score-based local color correction method to differentiate image pixels from ambiguity, resulting the segmentation quality to be highly improved. On the other hand, the privacy is assured by partially order homomorphic **Permutation Ordered Binary (POB)** number system and image permutation. Experiments are performed over publicly available images from the ISIC 2016 and 2017 challenges, as well as PH$^2$ dataset, where the proposed approach is found to achieve significant results over the encrypted images (known as encrypted domain), as compared to the existing schemes in the plain domain (unencrypted images). We also compare the results with the winners of the ISBI 2016 and 2017 challenges, and show that the proposed approach achieves a very close result with them, even after processing test images in the encrypted domain. Security of the proposed approach is analyzed using a challenge-response game model.

CCS Concepts: • **Security and privacy** → **Privacy protections**;

Additional Key Words and Phrases: Privacy-preservation, image segmentation, eHealth cloud application, multimedia security

**ACM Reference format:**
Amitesh Singh Rajput, Vishesh Kumar Tanwar, and Balasubramanian Raman. 2021. *Z*-Score-Based Secure Biomedical Model for Effective Skin Lesion Segmentation Over eHealth Cloud. *ACM Trans. Multimedia Comput. Commun. Appl.* 17, 2s, Article 65 (June 2021), 19 pages.
https://doi.org/10.1145/3430806

Authors' addresses: A. S. Rajput, Birla Institute of Technology and Science (BITS) Pilani, Pilani - 333031, Rajasthan, Pilani, India; email: amitesh.singh@pilai.bits-pilani.ac.in; V. K. Tanwar, Indian Institute of Technology Roorkee, Roorkee, India; email: vtanwar@ma.iitr.ac.in; B. Raman, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand, India; email: bala@cs.iitr.ac.in.

1551-6857/2021/06-ART65 $15.00
https://doi.org/10.1145/3430806

## 1 INTRODUCTION

The progressive advances being made with the application of computer to the area of bioscience and medicine have made a revolutionary change. According to *statista.com,*[1] a leading statistical prediction firm, the digital health market was 106 billion US dollars in 2019 and is expected to increase by six times, i.e., 639 billion US dollars by 2026. The advancement of eHealth has benefited various applications such as automatic computer analysis of pictures of biological and medical importance, special medical data processing methods, medical diagnosis, medical record processing, etc. Specifically, medical image segmentation has been emerging as one of the most useful systems, integrating the computer-based logic and medical sciences [12]. It consists of deploying specialized clustering techniques to find similar patterns in a patient's medical data obtained using electronic sensors.

Finding wide scope in various higher level applications such as medical imaging, image segmentation is the process of clustering similar pixels to get a more simplified representation, especially for analysis purpose [5, 36]. For example, automating the identification of cancerous area in a patient's dermoscopic image. To get a deeper insight, let us consider the problem arising due to Melanoma skin cancer. According to Gutman et al. [7], Melanoma skin cancer is one of the most fatal diseases that causes thousands of patients to lose their lives every year in the U.S. The medical experts are doing their best to provide any possible help and consultancy to the patients. However, due to a higher number of patients, some automated mechanism is required to help the doctors. In this situation, an on-demand cloud-based service seems a promising solution. The advantage includes cost-effective outsourcing of dermoscopic images for automatic processing on demand while removing the considerable burden of maintaining an in-house system from the user end (doctor/hospital). Also, one can clearly associate the progress being made by computers and the cloud for medical imaging in the current pandemic situation caused by Covid19, where significant need is raised for automatic remotely operated independent services. Since cloud-based remotely operated services seem a considerable way, they are assumed to be unreliable and users are always concerned when moving their personal data to the cloud [30, 33]. This is due to the fact that the cloud servers are developed and maintained by third parties, which may access user's data for certain benefits. The problem is further widened for medical images as they are a step ahead due to the containment of personal details of the patient [13]. We address this problems and propose a full-fledged privacy-preserving automatic dermoscopic image segmentation approach in this article.

The proposed approach is designed for efficient skin lesion segmentation using privacy-preserving *Z*-score-based automatic preprocessing and segmentation as a service. Here, in the viewpoint of privacy-preserving, we emphasize the security of the underlying dermoscopic image from third-party cloud server during storage and processing. The diverse security and privacy concerns surrounding medical data has been studied widely over the last few years and many organizations have published their reports [38] on the security and privacy issues for the manipulation of medical data in the networked systems. In the context of network security, the data privacy is assured using security protocols like HTTPS and SSL. However, the original data needs to be decrypted to the original form during processing at the cloud server. Due to this, securing the data content is of utmost importance before sending it to the cloud, which the proposed approach takes into better account. As a result, the underlying dermoscopic images are processed over the cloud server without requiring any intermediate decryption.

[1] https://www.statista.com/statistics/1092869/global-digital-health-market-size-forecast, accessed 09/10/20.

### 1.1 Technical Challenges and Their Resolution

Existing privacy-preserving multimedia computing schemes [15, 18, 25] primarily use **Homomorphic Encryption (HE)** for secure data processing. HE is a special form of encryption which allows specific computations to be performed over the encrypted data, such that, the decryption result matches the same operations being performed over the plain data. The existing HE schemes, such as Shamir's secret sharing [31], Paillier's cryptosystem [24], and others, support additive and scalar multiplicative operations. However, in the context of image segmentation, extensive comparison is required, which forms the challenging problem of incompatibility with the existing HE schemes. Also, the dermoscopic images are of large size and causes huge computational and storage overhead when used with the existing HE, requiring a resource efficient method.

On the other hand, since dermoscopic images are generated using electronic sensors, insufficient light and color effects are introduced. To avoid this problem, manual adjustments are required by an expert. In this situation, well-known automatic color correction techniques can be used. However, the existing color correction scheme, such as the pioneering method proposed by Moroney [19], is designed to process two-dimensional images captured using a digital camera and is found to be less effective when used as a preprocessing step for skin lesion segmentation. This is due to the fact that the pixel values lying near mean of the underlying image forms high ambiguity which affects the quality of the segmentation. This will be discussed in detail in Section 4.2. More precisely, the two major challenges that the proposed approach addresses and their resolution are described below.

- *Efficient Segmentation for Dermoscopic Images.* Since dermoscopic images are generated using electronic sensors, insufficient light and color effects are introduced. Also, as these images are obtained from an infected skin part, similarity between the affected area and the background skin forms high ambiguity which degrades the quality of segmentation. The problem is further widened when the difference between the foreground and background skin part is very minor. We address this challenge and provide an effective $Z$-score based preprocessing method to achieve efficient segmentation. The $Z$-score based preprocessing is the first attempt to define a virtual boundary, where pixel values lying near the mean of the underlying image are differentiated. This makes segmentation more efficient as the pixel ambiguity is resolved prior to processing.
- *Homomorphic Comparison.* In a generic methodology, the segmentation creates pixel clusters based on their color intensity values. However, the proposed work is intended to process dermoscopic images in the **Encrypted Domain (ED),** where pixel values are in encrypted form. Homomorphic encryption supports pixel processing in the encrypted domain for addition and multiplicative homomorphism. However, comparing pixel values in the ED for segmentation is a challenge that the proposed method addresses using **Permutation Ordered Binary (POB)** number system.

### 1.2 Contributions

Our objective is to design an efficient method such that the pixel values lying in the most ambiguous region of the underlying image can be differentiated. The proposed approach is a secure multi-disciplinary effort involving data clustering, medical imaging, privacy-preservation and cloud computing. The major contributions of this article are as follows:

(1) We propose a $Z$-score-based local color correction method. Due to this, the pixel intensity values lying near the mean of the underlying image are highly distinguished, resulting a better segmented image after processing.

(2) A partial order homomorphic POB number system is used for image encryption. As a result, the segmentation is efficiently achieved by keeping user privacy intact over the cloud.
(3) Upon comparison with the state-of-the-art schemes which performed the same task in the **Plain Domain (PD)** (where image content is visible), the proposed approach is designed to operate in the ED and still effective results are achieved.
(4) The security of the proposed approach is established using a challenge-response game model.

We review the literature advancement in the field of privacy-preserving data computing in Section 2, followed by preliminaries in Section 3. The proposed $Z$-score-based local color correction method and detailed functioning of the proposed approach is described in Section 4. Experimental result, comparison with the existing as well as winners of ISBI challenges and discussion is provided in Section 5. Performance assessment of the proposed approach is provided in Section 6. Section 7 provides its security analysis using a challenge-response game model. The article ends with a brief discussion regarding the future work and conclusion in Section 8.

## 2 RELATED WORK

During the past decade, various schemes have been proposed to address the growing demand of secure data computing. A few examples include secure collaborative recommendation [28], biometrics [14], multimedia distribution [16], data aggregation [42], confused modulo projection [11], data collection and offloading [2], and multi-secret image sharing [20]. Furthermore, certain medical-data-sharing-schemes are also available in the literature. These schemes include medical data transmission and analysis [8], medical data sharing [38] and medical records secure storage [3]. A good review of secure medical sharing schemes can be found at Jin et al. [10]. Considering the importance of data privacy and its underlying approaches, here, we review the state-of-the-art schemes in accord the *data anonymization, multi-party computation, differential privacy* and *cryptographic* techniques.

### 2.1 Data Anonymization

Data anonymization is among the well-known methods to protect data against identity disclosure [32]. It includes anonymizing the records so that certain individuals can become indistinguishable from each other. Nayahi and Kavitha [21] achieved this by utilizing the data clustering, and proposed to distribute the anonymized data set on a Hadoop distributed file system. Zhang et al. [44] addressed the scalability concerns related to big data anonymization for privacy assurance. The authors proposed a scalable two-phase top-down specialization approach to anonymize large-scale datasets using MapReduce framework on the cloud. Another effort for big data anonymization is found in Eyupoglu et al. [4], where the authors used chaos and perturbation techniques to assure data privacy.

### 2.2 Multi-Party Computation

**Multi-Party Computation (MPC)** is another method of secure data computing, where the research communities aim to process sensitive user's data partially over the cloud. It involves distributing the computation $C$ among $n$ number of participants in a manner, such that, none of the participants can get any information about the data. Akhter et al. [1] proposed a two-party-based secure $k$-means clustering method. The authors proposed an interactive protocol for processing $k$-means algorithm in a manner that two parties can process their data jointly without knowing any information about the individual data during. Gheid and Challal [6] proposed a privacy-preserving

$k$-means algorithm based on a multi-party additive scheme. However, instead of better results, their scheme required the involvement of $n$ parties, resulting in increased network overhead for practical scenario.

### 2.3 Differential Privacy

Differential privacy consists of adding random noise while maintaining certain statistical properties of the data [45]. Based on this principle, Ni et al. [22] proposed a secure multiple core DBSCAN clustering method for analysis of network user data. The authors used Laplacian noise iteratively and optimized the selection of initial core points to get superior results.

### 2.4 Cryptographic Methods

Instead of the data security mechanisms which are discussed above, a large group of research communities has adopted the Cryptographic methods that support HE. Patel et al. [26] proposed a privacy-preserving $k$-means scheme by utilizing Shamir's secret sharing. Initially, multiple data shares are generated which are further processed over different servers. The authors claimed that their scheme reduces computational cost. However huge communication and storage overhead is observed. A **Probabilistic C-Means (PCM)** algorithm for secure big data clustering was proposed by Zhang et al. [43]. The authors used a fully homomorphic **Brakerski-Gentry-Vaikunathan (BGV)** method for data security. An optimized high-order PCM method based on MapReduce for clustering big data has been developed. Xing et al. [37] proposed a novel approach for social participatory sensing using $k$-means clustering. Their scheme considered two privacy-preserving mechanisms, one for finding the nearest cluster and another for updating the cluster center. The authors used Paillier's cryptosystem [24] to secure user's data and shared it with a shared data analyst to accomplish the processing.

The above discussed methods achieved data privacy as per the requirement of the underlying situation. For example, Nayahi and Kavitha [21] emphasized data anonymization using utility preserving approach, whereas Zhang et al. [44] and Eyupoglu et al. [4] achieved the same using top-down specialization and chaos-perturbation techniques. Similarly, Akhter et al. [1] and Gheid and Challal [6] achieved secure $k$-means processing using a multi-party scheme. The similar trend can be observed for other two categories, that is, *Differential privacy* and *Cryptographic methods*. As these schemes have emphasized to perform the intended task, their demerits are considerable. For instance, the schemes using data anonymization, differential privacy, and cryptographic techniques suffer from huge computational complexity, whereas multi-party computation requires frequent communication between the entities involved. In this article, we consider these demerits and propose a secure dermoscopic image segmentation approach using partially homomorphic POB number system. As a consequence, the high computational and storage complexities are reduced and still privacy is achieved. Moreover, the intended task, i.e., secure segmentation is successfully performed over the encrypted images and superior results are achieved.

## 3 PRELIMINARIES

The preliminaries required to make this article self-contained are provided in this section.

### 3.1 POB Number System

As proposed by Sreekumar and Sundar [34], the POB number system consists of transforming a given number into a unique binary representation. The system is denoted by $POB(n, r)$, where $n$ and $r$ are positive integers such that $n > r$. Given a set of integers in the range $\{0, 1, \ldots \binom{n}{r} - 1\}$, this number system transforms each integer $i$ into a binary string of length $n$, known as a POB number $P_B = p_{n-1}, p_{n-2}, \ldots p_0$ with exactly $r$ 1's. The POB value $P_v$ corresponding to the POB number $P_B$ is evaluated as:

$$P_v = \sum_{i=0}^{n-1} p_i \binom{i}{r_i}, \ \ where \ \ r_i = \sum_{j=0}^{i} p_j. \tag{1}$$

The POB number $P_B$ and its corresponding POB value $P_v$ for a number $i$ is unique for each $(n, r)$. Therefore, if $n$ and $r$ are changed, the resulting $P_B$ and $P_v$ are also changed for the same number $i$. For example, the POB value corresponding to 15 for $n_1 = 9$ and $r_1 = 4$ is $P_{v_1}$=71, whereas it is completely changed to $P_{v_2}$=219 for $n_2 = 17$ and $r_2 = 6$. The properties of POB number system are described as follows:

(1) Given $(n, r)$ such that $n > r$, there will be exactly $\binom{n}{r}$ members in $POB(n, r)$ number system;
(2) POB representation is unique for each element in the range $\{0, 1, \ldots \binom{n}{r} - 1\}$.

These two properties form the primary base for the robustness achieved by the POB number system [33]. We utilize this number system to transform pixel intensity values of the underlying dermoscopic images in integration with pixel permutation. The security of our approach is assured by using a challenge-response game model in Section 7.

### 3.2 Color Correction

*Color correction* is the process of improving overall appearance of an image. In the context of dermoscopic images, it is one of the major aspects to be considered. The primary reason behind its consideration lies in the increased availability of medical imaging sensors which require effective preprocessing methods. Moroney [19] presented a pioneering work for color correction. The author proposed a novel tone reproduction scheme to enhance the contrast of digital images and named the term *local color correction*. However, it is infeasible to apply Moroney's method directly to dermoscopic images. The dermoscopic images are highly focused on the infected skin part and detailed information was not retained when we applied Moroney's scheme as a preprocessing step before segmentation. This is due to the fact that Moroney's scheme is designed to map higher and lower pixel intensity values into the mid-range intermediate band, which results in a visually appealing image for normal scenes. However, in the context of dermoscopic images, considerable ambiguity is introduced that causes poor segmentation. To overcome this problem, we propose a $Z$-score-based local color correction method. Our primary objective is to increase the inter-pixel difference lying near the mean, so that the ambiguity arising due to highly similar pixel values can be reduced. The proposed method is discussed in detail in Section 4.

## 4 PROPOSED *Z*-SCORE-BASED LOCAL COLOR CORRECTION

In this section, we first provide a brief overview of the proposed approach, followed by the detailed description of its functions and methodology in the next subsections.

### 4.1 System Overview

We consider an eHealth cloud environment and classify the functioning operations of the proposed method as per the trust server and cloud server modalities. The trust server is described as an independent user-accessible device, facilitating multimedia preprocessing and encryption operations. The remaining operations, that is, secure storage and processing for effective image segmentation are performed at cloud server. This is accomplished by deploying a secure image segmentation model over the eHealth cloud, soliciting the task of privacy-preserving image segmentation remotely.

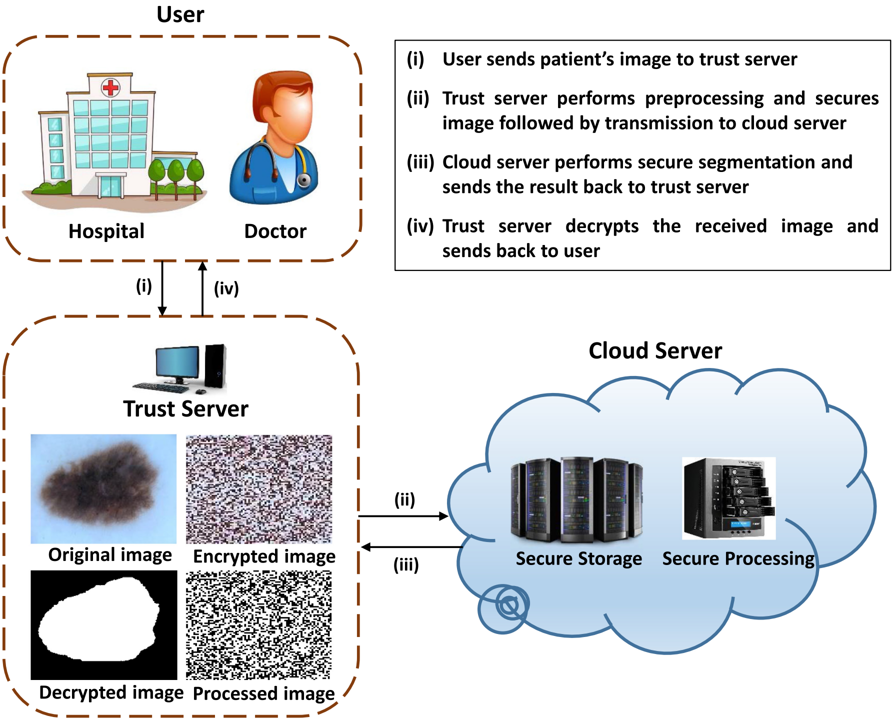

User
Hospital
Doctor
(i) User sends patient's image to trust server
(ii) Trust server performs preprocessing and secures image followed by transmission to cloud server
(iii) Cloud server performs secure segmentation and sends the result back to trust server
(iv) Trust server decrypts the received image and sends back to user
(i)
(iv)
Trust Server
Original image
Encrypted image
Decrypted image
Processed image
(ii)
(iii)
Cloud Server
Secure Storage
Secure Processing

Fig. 1. Overview of the proposed approach.

The architecture we propose is based on "honest-but-curious" adversary model, wherein the cloud server executes the desired task, however is eager to know about the data content. According to Paverd et al. [27], "the honest-but-curious adversary is a legitimate participant in a communication protocol who will not deviate from the defined protocol but will attempt to learn all possible information from legitimately received messages". In the context of cloud computing, we use this terminology to represent a legitimate cloud server which honestly performs all the assigned tasks, however, is curious to know about the data content. Due to this, the image information is secured before transmitting to the cloud server in a manner, such that, the cloud server can perform the desired task; however, it would not get any information related to privacy content in the data. The data is secured by POB number system and image permutation, and the cloud server is directed to perform storage processing operations over the encrypted image. Due to this, the disclosure of user's personal information is completely avoided over the cloud. An overview of the proposed approach is shown in Figure 1.

## 4.2 Functions Used

The functions used in the proposed approach are defined as follows:

- ***CenCrop(I)***: This function performs center cropping over the input image *I* for more meaningful representation. Due to this, the unnecessary image regions are removed, resulting a more informative image.
- ***Disk(I)***: It takes an input image *I* and performs disk filtering. The disk filter removes unwanted hair streaks in dermoscopic images so that smooth functioning can be achieved.

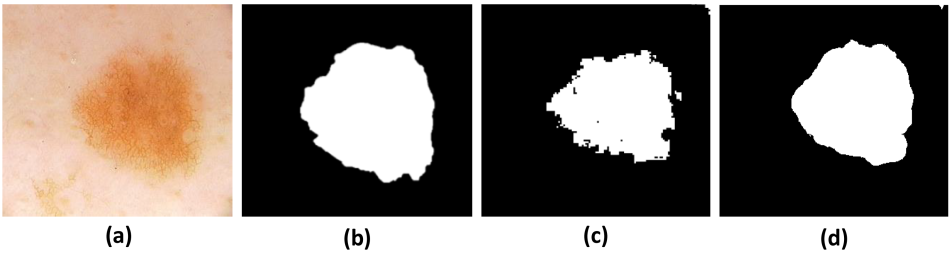


Fig. 2. Analysis of segmentation effects; (a) Original image, (b) Ground truth, (c) Segmentation using Moroney's scheme [19], and (d) Segmentation using $Z$-score-based preprocessing.

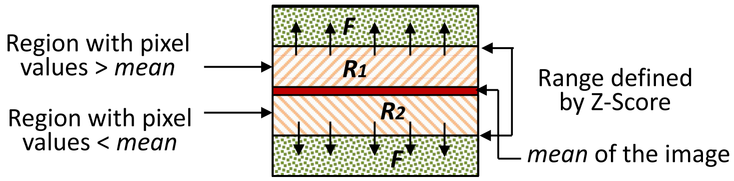
- ***Per(I, $k_1$)***: Here, pixel values of the given image $I$ are permuted according to the shuffling sequence generated from a secret key $k_1$. To achieve this, we use the same pixel permutation method proposed in [29]. As a result, a permuted image $I_p$ is obtained as output of this step.
- ***POB($I_i$, n, t)***: It takes pixel value at location $i$ in image $I$ and transforms it to the corresponding POB value $P_v$ using security parameters $n$ and $t$. The security parameters $n$ and $t$ forms another secret key $k_2$.

As discussed in the previous section, the functions *CenCrop* and *Disk* are designed to preprocess the underlying image $I$, whereas *Per* and *POB* are specific to image encryption. The *CenCrop* and *Disk* performs center cropping and hair removal over $I$. However, the image tone remains unchanged which forms an important preprocessing requirement, especially for dermoscopic images. Dermoscopic images are generated through electronic sensors and are focused towards the infected body part. Due to high ambiguity between background skin and the infected part, and the use of electronic sensors to generate the dermoscopic image, it has been found that the quality of segmentation is reduced if we directly process the underlying dermoscopic image; thus, requiring manual adjustments by an expert. To automate the process of color correction, the well-known Moroney's local color correction scheme [19] can be adopted. However, when we directly implemented it over the dermoscopic image as a preprocessing step, the quality of segmentation is reduced. The resulting image is shown in Figure 2(c), where poor segmentation, obtained by directly using Moroney's scheme is depicted for its original and ground truth in Figures 2(a) and 2(b). To overcome this problem, we propose a $Z$-score-based preprocessing method.

Considering the dermoscopic images, the proposed method is designed in a manner, such that, the inter-pixel difference lying near the mean of the image can be increased. Initially, the range of pixel values that need to be considered for this purpose is identified using a $Z$-score. These pixel values are then processed for color correction. As a consequence, the ambiguity due to highly similar pixel values near the mean of the image is reduced. The resulting image is shown in Figure 2(d), where significant improvement can be observed. An illustration of the proposed $Z$-score-based method is shown in Figure 3, where pixel intensity values lying in the range ($R_1$ and $R_2$) defined by $Z$-score are modified for color correction with inclination towards the suitable region ($F$). The complete methodology is described in Algorithm 1. For brevity reasons, only one color channel is considered. Although, the same methodology is applied over other color channels of the image. A working example of the proposed method is demonstrated in Figure 4, where $\mu$ and $\sigma$ depicts the mean and standard deviation of the image.

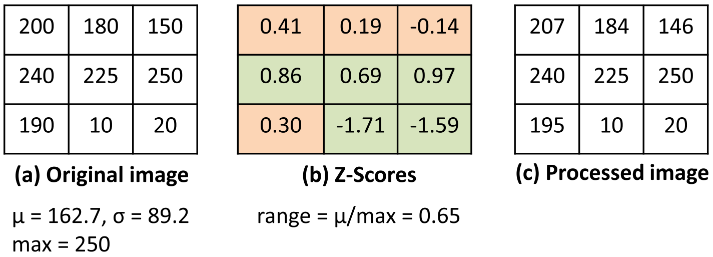
### 4.3 Privacy-Preserving Image Segmentation-as-a-Service

The two primary objectives of the proposed approach consist of: (i) preprocessing and securing image content at trust server, and (ii) performing image segmentation over the cloud. The complete


Region with pixel values > *mean*
Region with pixel values < *mean*
F
R1
R2
F
Range defined by Z-Score
*mean* of the image

* F depicts the region containing pixels suitable for segmentation

Fig. 3. Proposed *Z*-score-based color correction.



| | | |
|---|---|---|
| 200 | 180 | 150 |
| 240 | 225 | 250 |
| 190 | 10 | 20 |

**(a) Original image**

μ = 162.7, σ = 89.2
max = 250

| | | |
|---|---|---|
| 0.41 | 0.19 | -0.14 |
| 0.86 | 0.69 | 0.97 |
| 0.30 | -1.71 | -1.59 |

**(b) Z-Scores**

range = μ/max = 0.65

| | | |
|---|---|---|
| 207 | 184 | 146 |
| 240 | 225 | 250 |
| 195 | 10 | 20 |

**(c) Processed image**

Fig. 4. Working example of the proposed method. Orange blocks represent pixels that need to be processed (identified by *Z*-score), whereas green depicts no processing.

**ALGORITHM 1:** *Z*-score based local color correction

```
Input: Test image $\mathcal{G}$                          ▷ One color channel
Output: Local color corrected image
Evaluate mean ($\mu$) and standard deviation ($\sigma$) of $\mathcal{G}$
$\vartheta = max(\mathcal{G})$                           ▷ Find maximum pixel intensity value of $\mathcal{G}$
$\gamma = \mu/\vartheta$;                                ▷ Range in which pixel values are processed
$i = 1$
while $i \leq k$ do                                      ▷ $k$ is the total number of pixels in $\hat{\mathcal{G}}$
    $Z_i = \frac{\mathcal{G}_i - \mu}{\sigma}$           ▷ Evaluate $Z$-score of pixel $i$
    if ($Z_i \leq \gamma$ && $Z_i > (-\gamma)$) then
        $\phi = 2^{\frac{\mu - \mathcal{G}}{\mu}}$
        $\hat{\mathcal{G}}_i = \left(\frac{\mathcal{G}_i}{\vartheta}\right)^{\phi} \times \vartheta$
    end if
    $i = i + 1$;
end while
```

working steps describing image preprocessing and encryption at trust server is provided in Algorithm 2 (for one color channel). The image preprocessing consists of center cropping, disk filtering and *Z*-score based local color correction, whereas the security is achieved by pixel permutation followed by modification of pixel intensity values using POB number system.

Upon receiving the encrypted image $\hat{E}$, it is the duty of the cloud server to perform secure segmentation and return the processed image back to the trust server. For segmentation, we use *k*-Means clustering algorithm over the cloud. The reason for selecting *k*-Means clustering algorithm is due to the fact that the proposed method is designed to increase the difference among pixel values lying near image's mean. On the other hand, the *k*-Means algorithm performs data clustering based

**ALGORITHM 2:** Image preprocessing and encryption at trust server

```
Input: Secret image $S$                                          ▷ dermoscopic image
Output: Encrypted image $E$
$\mathcal{C} = CenCrop(\mathcal{S})$                             ▷ Remove unwanted information
$\mathcal{D} = Disk(\mathcal{C})$                                ▷ Remove unwanted hair streaks
Perform local color correction using proposed methodology in Section 4.
Let $\hat{\mathcal{G}}$ represents local color corrected image obtained in the previous step, secure its pixel
intensity values as follows
$\mathcal{P} = Per(\hat{\mathcal{G}}, k_1)$                      ▷ Permute pixels of $\hat{\mathcal{G}}$ using secret key $k_1$
$i = 1$;
while $i \leq k$ do                                              ▷ $k$ is the total number of pixels in $\mathcal{P}$
    $E_i = POB(\mathcal{P}_i, n, t)$                             ▷ Pixel modification using POB
    $i = i + 1$;
end while
The encrypted image $E$ consists of large numbers due to the application of POB number sys-
tem, normalize its pixel intensity values in the range [0,255] as follows.
$E_{min} = min(E)$                                               ▷ Minimum value of $E$
$E_{max} = max(E)$                                               ▷ Maximum value of $E$
$j = 1$;
while $j \leq k$ do                                              ▷ $k$ is the total number of pixels in $E$
    $\hat{E}_j = \left(\frac{E_j - E_{min}}{E_{max} - E_{min}}\right) \times 255$        ▷ Normalized pixel value
    $j = j + 1$;
end while
Transmit $\hat{E}$ to cloud server.
```

on mean values and fits in the scenario. Once processed, the trust server accesses the processed image and decrypts it. The decryption simply follows pixel reshuffling to restore them to their original position and reversing the POB values using secret keys $k_1$ and $k_2$, respectively.

## 5 EXPERIMENTAL RESULTS

In this section, we assess the segmentation quality achieved by the proposed approach in the ED, and compare it with the existing as well as state-of-the-art methods.

### 5.1 Dataset

Experiments are performed over a variety of images, obtained from three different datasets. The first dataset consists of 900 and 379 dermoscopic images provided by the International Skin Imaging Collaboration (ISIC), to be used as the training and testing sets in the challenge of “Skin Lesion Analysis toward Melanoma Detection” at the International Symposium on Biomedical Imaging (ISBI 2016) [7]. The second dataset is an extension of ISBI 2016 images, contributing a total of 2000 and 600 training and testing images, known as ISBI 2017. The third dataset, named as PH$^2$, consists of 200 dermoscopic images acquired at the Dermatology Service of Hospital Pedro Hispano, Matosinhos, Portugal and was provided by Mendonca et al. [17]. The ground truth segmentation of the lesion in each category is available in all the datasets as well. To reduce the computational overhead during experimentation, the images are resized to 400 × 400 and then processed.

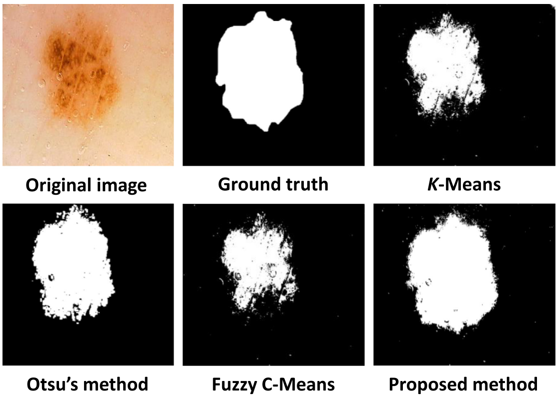


Fig. 5. Comparison of the proposed approach with existing schemes over ambiguous pixels.

## 5.2 Comparison with Well-Known Existing Schemes

Here, the proposed approach is employed to perform skin lesion segmentation over all images of the selected datasets and the quality of resulting images is compared with the well-known existing schemes including *k-Means*, *Otsu's method,* and *Fuzzy C-Means* clustering. Upon comparison, it has been found that the proposed approach performs significantly better for images with a higher level of ambiguity among pixel intensity values. Figure 5 depicts this situation, where higher ambiguity among skin color and infected part can be observed in the original dermoscopic image. Due to this, the existing image segmentation schemes are found to possess poor segmentation. On the other hand, the proposed approach differentiates image colors using *Z*-score-based local color correction and then processes the modified image for secure segmentation. As a result, efficient segmentation quality is achieved.

In addition to the significant improvement achieved by the proposed approach over ambiguous pixel intensity values, the resulting images are found to be superior when assessed over normal dermoscopic images. A few sample images are shown in Figure 6, where superiority of the proposed approach can be clearly observed. All inclusive, in spite of higher noise level in the ED, the proposed approach is found to possess superior results as compared to the existing schemes, which processes image pixels directly in the PD.

*5.2.1 Evaluation Based on Similarity Metrics.* For statistical assessment, we use the evaluation metrics that are suggested in the ISBI 2016 challenge for benchmarking. These metrics include Dice Coefficient (DC), Jaccard Index (JI), Sensitivity (SE), Specificity (SP), and Accuracy (AC). The metrics are defined as follows:

$$\begin{aligned} DC &= 2TP/(2TP + FN + FP) \\ JI &= TP/(TP + FN + FP) \\ SE &= TP/(TP + FN) \\ SP &= TN/(TN + FP) \\ AC &= (TP + TN)/(TP + FP + TN + FN) \end{aligned} \tag{2}$$

where TP, TN, FP, and FN refers the number of true positives, true negatives, false positives, and false negatives, respectively.

We assess the proposed approach with the above-mentioned evaluation metrics and found its resulting scores to be highly improved. The average resulting scores achieved by the proposed approach and their comparison with the existing schemes are shown in Tables 1, 2, 3, 4, and 5

Table 1. Comparison with Existing Schemes for Training Images of ISBI 2016 Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| *k-Means* | 0.60 | 0.48 | 0.74 | 0.88 | 0.81 |
| *Otsu's* | 0.61 | 0.50 | **0.79** | 0.84 | 0.81 |
| *FCM* | 0.62 | 0.49 | 0.73 | 0.88 | 0.81 |
| *Proposed method* | **0.80** | **0.69** | 0.75 | **0.93** | **0.82** |

Table 2. Comparison with Existing Schemes for Testing Images of ISBI 2016 Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| *k-Means* | 0.62 | 0.50 | 0.74 | 0.89 | 0.82 |
| *Otsu's* | 0.61 | 0.50 | **0.79** | 0.84 | 0.80 |
| *FCM* | 0.63 | 0.51 | 0.73 | 0.89 | 0.82 |
| *Proposed method* | **0.80** | **0.71** | 0.76 | **0.92** | **0.83** |

Table 3. Comparison with Existing Schemes for Training Images of ISBI 2017 Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| *k-Means* | 0.58 | 0.45 | 0.78 | 0.90 | 0.84 |
| *Otsu's* | 0.58 | 0.46 | **0.84** | 0.86 | 0.83 |
| *FCM* | 0.57 | 0.45 | 0.77 | 0.89 | 0.84 |
| *Proposed method* | **0.78** | **0.67** | 0.79 | **0.94** | **0.84** |

Table 4. Comparison with Existing Schemes for Testing Images of ISBI 2017 Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| *k-Means* | 0.61 | 0.49 | 0.77 | 0.90 | 0.84 |
| *Otsu's* | 0.62 | 0.50 | **0.80** | 0.87 | 0.83 |
| *FCM* | 0.59 | 0.47 | 0.76 | 0.90 | 0.83 |
| *Proposed method* | **0.77** | **0.66** | 0.76 | **0.91** | **0.84** |

Table 5. Comparison with Existing Schemes for Images of PH$^2$ Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| *k-Means* | 0.68 | 0.53 | 0.77 | 0.86 | 0.83 |
| *Otsu's* | 0.74 | 0.61 | **0.89** | 0.84 | 0.85 |
| *FCM* | 0.65 | 0.51 | 0.74 | 0.86 | 0.82 |
| *Proposed method* | **0.88** | **0.79** | 0.83 | **0.92** | **0.86** |

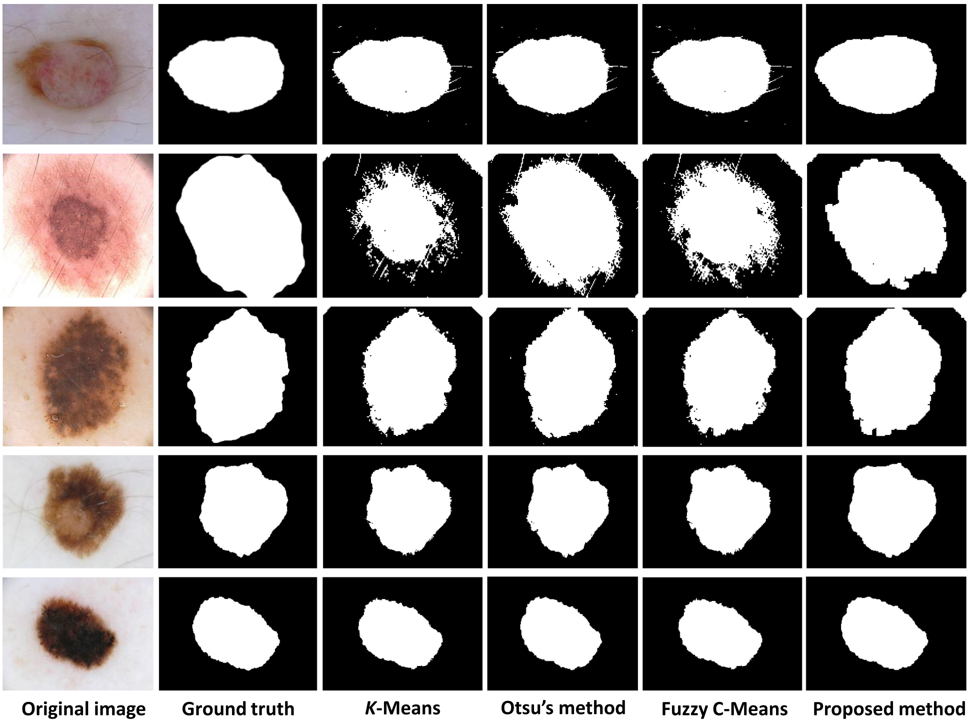


Fig. 6. Comparison of the proposed approach with existing schemes over normal pixels.

Table 6. Comparison with Winners of ISBI 2016 Challenge for Testing Images of ISBI 2016

| Method | DC | JI | SE | SP | AQ | Data privacy |
|---|---|---|---|---|---|---|
| Yuan et al. [40] | 0.91 | 0.84 | 0.91 | 0.96 | 0.95 | × |
| Yu et al. [39] | 0.89 | 0.82 | 0.91 | 0.95 | 0.94 | × |
| Tajeddin et al. [35] | 0.88 | 0.81 | 0.83 | 0.98 | 0.94 | × |
| *Proposed method* | 0.80 | 0.71 | 0.76 | 0.92 | 0.83 | ✓ |

for training and testing images of ISBI 2016 and 2017 challenge datasets, and with images of PH$^2$ dataset, respectively.

### 5.3 Comparison with the Winners of ISBI Challenges

We compare the proposed approach with the winners of the ISBI challenges which performed the intended task in the PD. The average statistical scores reported by the winners over images of ISBI 2016 challenge (testing data) is found to be in the range $0.88 - 0.91, 0.81 - 0.84, 0.83 - 0.91, 0.96 - 0.98$, and $0.94 - 0.95$ for DC, JI, SE, SP, and AQ, respectively. On the contrary, the proposed approach is designed to process encrypted images, and still close results are achieved. The comparison is shown in Table 6. The similar fact is observed when compared with the winners of ISBI 2017 dataset in Table 7, where the proposed approach is found to possess very close scores, even after processing the underlying images in the ED.

Table 7. Comparison with Winners of ISBI 2017 Challenge for Testing Images of ISBI 2017

| Method | DC | JI | SE | SP | AQ | Data privacy |
|---|---|---|---|---|---|---|
| Yuan et al. [41] | 0.84 | 0.76 | 0.82 | 0.97 | 0.93 | × |
| Jahanifar Zamani et al. [9] | 0.83 | 0.74 | 0.81 | 0.98 | 0.93 | × |
| Tschandl et al. [36] | 0.85 | 0.76 | - | - | - | × |
| *Proposed method* | 0.77 | 0.66 | 0.76 | 0.91 | 0.84 | ✓ |

Table 8. Difference between Scores Obtained by the Winners of ISBI 2016 Challenge (PD) and the Proposed Method (ED) for Testing Images of ISBI 2016 Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| Yuan et al. [40] | 0.11 | 0.13 | 0.15 | 0.04 | 0.12 |
| Yu et al. [39] | 0.09 | 0.11 | 0.15 | 0.03 | 0.11 |
| Tajeddin and Asl [35] | 0.08 | 0.10 | 0.07 | 0.06 | 0.11 |
| *Average* | 0.09 | 0.11 | 0.12 | 0.04 | 0.11 |

### 5.4 Discussion

The usual preprocessing techniques for dermoscopic image consist of *Center cropping* and *Hair removal.* As the name suggests, the first method performs center cropping over the input image $I$ for more meaningful representation by removing unnecessary image regions. The later method is a disk filter that removes unwanted hair streaks in dermoscopic images. However, despite of these existing preprocessing techniques, the image tone remains unchanged which forms an important preprocessing requirement. As the dermoscopic images are emphasized to an infected skin part, the similarity between affected area and the background skin forms high ambiguity which degrades the quality of segmentation. We address this problem and provide an effective $Z$-score-based preprocessing method to achieve efficient segmentation. The $Z$-score-based preprocessing is the first attempt to define a virtual boundary, where pixel values lying near the mean of the image are differentiated. This makes segmentation more efficient as the ambiguity is resolved prior processing. As a consequence, the proposed method is found to be superior when compared to the well-known existing schemes: *k-Means, Otsu's method,* and *Fuzzy C-Means* clustering.

On the other hand, as compared to the winners of the ISBI 2016 and 2017 challenges in Tables 6 and 7, the proposed method is slightly degrading at the cost of privacy. Here, it is important to note that the previous methods processed underlying images in the plain-form (PD), where image content is visible, and were selected as the best in their respective challenges. However, the proposed method is designed to work in the secured domain (ED), where the underlying images are processed in the encrypted form. This forms a significant advancement in today's world, where the required service can be availed on-demand anytime and anywhere without compromising the data privacy. On the other hand, while assessing the segmentation quality, it has been found that the degradation is very less at the cost the privacy. Please refer to Tables 8 and 9, where the difference between scores obtained by the winners of ISBI 2016 and 2017, and the proposed method is shown, respectively. For convenience in understanding, the average scores are computed and depicted in the last row, where negligible difference for all the parameters can be observed.

## 6 PERFORMANCE ANALYSIS

The complexity of the proposed approach is dependent on the computation of four sub-processes, namely, $Z$-score and other preprocessing methods, image encryption, *k-Means* clustering for

Table 9. Difference between Scores Obtained by the Winners of ISBI 2017 Challenge (PD) and the Proposed Method (ED) for Testing Images of ISBI 2017 Dataset

| Method | DC | JI | SE | SP | AQ |
|---|---|---|---|---|---|
| Yuan and Lo [41] | 0.07 | 0.10 | 0.06 | 0.06 | 0.09 |
| Jahanifar et al. [9] | 0.06 | 0.08 | 0.05 | 0.07 | 0.09 |
| Tschandl et al. [36] | 0.08 | 0.10 | - | - | - |
| *Average* | 0.07 | 0.09 | 0.06 | 0.06 | 0.09 |

Table 10. Analysis of Computational Time for Varying Images of Different Size, Processed by the Proposed Approach (Time is Shown in Seconds)

| Image size | Preprocessing | Encryption | Segmentation | Decryption | Total time |
|---|---|---|---|---|---|
| 128 × 128 | 0.013 | 0.015 | 0.011 | 0.002 | 0.041 |
| 256 × 256 | 0.041 | 0.064 | 0.049 | 0.008 | 0.162 |
| 512 × 512 | 0.192 | 0.240 | 0.147 | 0.031 | 0.610 |
| 1024 × 1024 | 0.735 | 0.911 | 0.935 | 0.121 | 2.702 |

segmentation, and decryption. For instance, the computation time for a 256 × 256 skin lesion image (RGB) over a desktop PC with Intel i5-7200U @2.50GHz processor with 8 GB RAM is 0.041 seconds for preprocessing, 0.064 seconds for encryption, 0.049 seconds for segmentation, and 0.008 seconds for decryption, making a total of 0.162 seconds. The same computation for different images of varying sizes, processed by the proposed approach, is shown in Table 10. On the other hand, comparing this computation with other methods that are indicated in Tables 6 and 7 would be unfair as they differ in many aspects which are described below.

- The existing schemes shown in Tables 6 and 7 are data-driven approaches, especially built using deep convolutional neural networks (deep CNNs), whereas our scheme processes a single image at a time without explicitly considering any learning data.
- Considering the advantage of data visibility in the PD, pixel inter-correlation is utilized in existing schemes to generate a dense feature representation of input image, whereas the proposed method uses an entirely encrypted image with no association between adjacent pixels in the ED.
- Massive data collection is required by the existing schemes to fulfill the requirements of the underlying scenario. Every health organization may not fulfill this requirement as training over a large dataset is a bit complex. On the contrary, the proposed approach requires only one image at a time and does the intended job. This saves significant data collection efforts, making the proposed method a step ahead as compared to the existing schemes.
- With reference to the previous point in the context of resource utilization, the existing schemes require highly configured computational and storage resources. On the contrary, since the proposed method is designed to directly execute the underlying images (in encrypted form) without requiring any explicit training dataset, the need of rich resources is significantly reduced.

Ozturk and Ozkaya [23] depict the average training and testing time for different skin lesion segmentation models (in the PD where image content is processed without encryption) as shown in Table 11. According to Ozturk and Ozkaya [23], the test time should be less than 10 seconds for

Table 11. Performance of the Training and Testing Time for Various Skin Lesion Segmentation Models, Ozturk et al. [23] (Time is Shown in Seconds)

| Models | Training time per epoch | Test time per image |
|---|---|---|
| U-Net | 486.6 | 8.1 |
| SegNet | 464.8 | 8.3 |
| FCN | 465.6 | 9.7 |
| FrCN | 395.2 | 7.6 |
| iFCN | 432.3 | 8.0 |

dermoscopic images. With reference to this constraint, the proposed approach avoids the need of explicit training and achieves optimized performance (even for a high-dimension encrypted image of size 1024 × 1024) as compared to the testing time of existing schemes as depicted in Table 11. This makes the proposed approach a suitable candidate for practical scenario.

## 7 SECURITY ANALYSIS

The proposed approach assures security of the image data based on POB number system. The security of this cryptosystem is dependent on two key parameters $(n, r)$. Additionally, we used image shuffling to permute image pixels before transmission. Here, we discuss the security strengths of the proposed approach using a challenge response game model.

### 7.1 Challenge Response Game Model

The game consists of a challenger $C$ and a Probabilistic Polynomial Time adversary $\mathcal{A}$, asking for $n$ number of decryptions from $C$. Once received, the adversary $\mathcal{A}$ then evaluates to decrypt a new ciphertext. We consider the trust server as challenger and cloud server as adversary, and describe the game as follows;

**Game 1:** The challenger $C$ initially generates its secret key parameters $(n, r)$ and encrypts a secret message $m$. Let $[\![m]\!]$ represents the encrypted message, the challenger $C$ sends it to $\mathcal{A}$. The adversary $\mathcal{A}$ then receives $[\![m]\!]$, and generates its own arbitrary messages $\{m_1, m_2, \ldots, m_t\}$ with their corresponding $\{(n_1, r_1), (n_2, r_2), \ldots, (n_t, r_t)\}$, and sends them to $C$ for their encryptions. The challenger $C$ then encrypts the received messages $\{m_1, m_2, \ldots, m_t\}$ with their corresponding key parameters $\{(n_1, r_1), (n_2, r_2), \ldots (n_t, r_t)\}$, and transmits the encrypted messages $\{[\![m_1]\!], [\![m_2]\!], \ldots [\![m_t]\!]\}$ back to $\mathcal{A}$. The adversary $\mathcal{A}$ then randomly selects an encrypted message $[\![m_i]\!]$ and asks $C$ for its decryption using its own $(n, r)$. The challenger $C$ then decrypts $[\![m_i]\!]$ using its own $(n, r)$, and sends the result (say $m_i$) to $\mathcal{A}$. Upon receiving $m_i$, the adversary $\mathcal{A}$ then decrypts the same encrypted message with its own $(n_i, r_i)$ to get $\hat{m}_i$ such that any association between $m_i$ and $\hat{m}_i$ can be found. Under this scenario, the POB number system is found to be highly secure with probability of being $Pr(m_i = \hat{m}_i)$ as negligible.

Theorem 1. *A secret message $m$ when secured using POB number system with sufficiently large $(n, r)$ is highly secure.*

Proof. Since each digit of a POB number (say $b_j$) is associated with its position value, the value represented by POB number $P_B$ is unique for each of its input. Let us consider a secret message $m$, and encrypt it using $(n_1, r_1)$ to get $[\![m_1]\!]$. Now, if we encrypt the same message $m_1$ with slightly different key parameters say $(n_2, r_2)$ to get $[\![m_2]\!]$, the probability of being $Pr([\![m_1]\!] = [\![m_2]\!])$ is negligible. This is due to the fact that the range of POB number lies between $[0, \binom{n}{r} - 1]$. Therefore, for sufficiently large $(n, r)$, the probability that $[\![m]\!]$ can be any value from the set $A = \{0, 1, \ldots T\}$, $T = \binom{n}{r} - 1$, is given as

$$Pr([\![m]\!]) = \frac{1}{T} \tag{3}$$

Here, it is important to note that $T$ is completely dependent on $n$ and $r$. Thus, for sufficiently large $(n_1, r_1)$ and $(n_2, r_2)$, the probability of being $[\![m_1]\!]$=$[\![m_2]\!]$ is negligible implying that if an adversary wants to extract original secret message $m$ from $[\![m_1]\!]$ (or $[\![m_2]\!]$) using irrelevant key parameters $(n_2, r_2)$ (or $(n_1, r_2)$), it is almost impossible. For instance, refer to Corollary 1. □

Corollary 1. *In particular, for* $n_1 = 21$ *and* $r_1 = 15$*, the total number of POB values are 54263, i.e.,* $T = 54263$ *(say* $T_1$*). Therefore, the probability of an encrypted message* $[\![m]\!]$ *of being any value from the set in the range* $[0, \binom{n_1}{r_1} - 1]$ *is given by* $Pr([\![m]\!]) = 1.8429 \times 10^{-5}$*. Now, if we slightly downgrade* $r_1 = 15$ *to* $r_2 = 14$ *to make a new key parameter* $(n_2 = 21, r_2 = 14)$*, the total number of POB values* $(T_2)$ *changes to 116279. In this case,* $Pr([\![m]\!])$ *becomes* $8.6000 \times 10^{-6}$*. Similarly, if we slightly upgrade* $r_1 = 15$ *to* $r_3 = 16$ *to make a new key parameter* $(n_3 = 21, r_3 = 16)$*, the new count for total number of POB values* $(T_3)$ *becomes 20348, with* $Pr([\![m]\!])$ *as* $4.9145 \times 10^{-5}$.

Therefore, it can be clearly observed that there is a huge distinction between the probabilities of $[\![m]\!]$ being any value from the set of resulting numbers when $(r)$ is slightly changed. The same distinction can be experienced with varying the values of $n$. Also, this difference is significantly increased when moving to other higher values of $(n, r)$. The proposed methodology considers dermoscopic images as the secret and secures its pixel intensity values using POB number system. Moreover, the pixel values are shuffled also, which forms another layer of security.

## 8 CONCLUSION

In this article, a privacy-preserving image segmentation approach has been proposed. We have emphasized the feasibility to perform effective and secure image segmentation by proposing a *Z*-score based local color correction method. Initially, scope of the proposed method has been discussed along with the existing works in the field of secure data clustering. Next, image preprocessing is described using the proposed *Z*-score based local color correction method, followed by securing image information using the POB number system and image permutation. As a result, effective segmentation is achieved with complete privacy assurance. Moreover, the proposed approach is tested over different images of ISBI 2016, 2017, and PH$^2$ datasets, and is found to be highly effective against existing as well as state-of-the-art schemes. All inclusive, a secure and practical approach has been designed for outsourcing the considerable burden of medical image segmentation remotely, and superior results are achieved. In the future, the proposed approach can be extended for other data processing tasks in the ED.

## REFERENCES

[1] Rahena Akhter, Rownak Jahan Chowdhury, Keita Emura, Tamzida Islam, Mohammad Shahriar Rahman, and Nusrat Rubaiyat. 2013. Privacy-preserving two-party k-means clustering in malicious model. In *Proceedings of the IEEE 37th Annual Computer Software and Applications Conference Workshops*. 121–126.

[2] Siguang Chen, Xi Zhu, Haijun Zhang, Chuanxin Zhao, Geng Yang, and Kun Wang. 2020. Efficient privacy preserving data collection and computation offloading for fog-assisted IoT. *IEEE Transactions on Sustainable Computing* (2020).

[3] Yi Chen, Shuai Ding, Zheng Xu, Handong Zheng, and Shanlin Yang. 2019. Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems* 43, 1 (2019), 5.

[4] Can Eyupoglu, Muhammed Aydin, Abdul Zaim, and Ahmet Sertbas. 2018. An efficient big data anonymization algorithm based on chaos and perturbation techniques. *Entropy* 20, 5 (2018), 373.

[5] Haidi Fan, Fengying Xie, Yang Li, Zhiguo Jiang, and Jie Liu. 2017. Automatic segmentation of dermoscopy images using saliency combined with Otsu threshold. *Computers in Biology and Medicine* 85 (2017), 75–85.

[6] Zakaria Gheid and Yacine Challal. 2016. Efficient and privacy-preserving k-means clustering for big data mining. In *Proceedings of the IEEE Trustcom/BigDataSE/ISPA*. 791–798.

[7] David Gutman, Celebi Emre Codella, Noel C. F. Marchetti, Michael Helba Brian, and Allan Halpern Mishra Nabin. 2016. Skin lesion analysis toward melanoma detection: A challenge at the International Symposium on Biomedical Imaging (ISBI) 2016, hosted by the International Skin Imaging Collaboration (ISIC). In [Online]. Available: https://arxiv.org/abs/1605.01397.

[8] Haiping Huang, Tianhe Gong, Ning Ye, Ruchuan Wang, and Yi Dou. 2017. Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Transactions on Industrial Informatics* 13, 3 (2017), 1227–1237.

[9] Mostafa Jahanifar, Neda Zamani Tajeddin, Babak Mohammadzadeh Asl, and Ali Gooya. 2019. Supervised saliency map driven segmentation of lesions in dermoscopic images. *IEEE Journal of Biomedical and Health Informatics* 23, 2 (2019), 509–518.

[10] Hao Jin, Yan Luo, Peilong Li, and Jomol Mathew. 2019. A review of secure and privacy-preserving medical data sharing. *IEEE Access* 7 (2019), 61656–61669.

[11] Xin Jin, Hongyu Zhang, Xiaodong Li, Haoyang Yu, Beisheng Liu, Shujiang Xie, Amit Kumar Singh, and Yujie Li. 2020. Confused modulo projection based somewhat homomorphic encryption-cryptosystem, library and applications on secure smart cities. *IEEE Internet of Things Journal* (2020).

[12] Pratik Kalshetti, Manas Bundele, Parag Rahangdale, Dinesh Jangra, Chiranjoy Chattopadhyay, Gaurav Harit, and Abhay Elhence. 2017. An interactive medical image segmentation framework using iterative refinement. *Computers in Biology and Medicine* 83 (2017), 22–33.

[13] R. Karakış, İ. Güler, İ. Çapraz, and E. Bilir. 2015. A novel fuzzy logic-based image steganography method to ensure medical data security. *Computers in Biology and Medicine* 67 (2015), 172–183.

[14] Santosh Kumar, Sanjay Kumar Singh, Amit Kumar Singh, Shrikant Tiwari, and Ravi Shankar Singh. 2018. Privacy preserving security using biometrics in cloud computing. *Multimedia Tools and Applications* 77, 9 (2018), 11017–11039.

[15] Ankita Lathey and Pradeep K. Atrey. 2015. Image enhancement in encrypted domain over cloud. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 11, 3 (2015), 38.

[16] David Megías and Amna Qureshi. 2017. Collusion-resistant and privacy-preserving P2P multimedia distribution based on recombined fingerprinting. *Expert Systems with Applications* 71 (2017), 147–172.

[17] Teresa Mendonça, Pedro M. Ferreira, Jorge S. Marques, André R. S. Marcal, and Jorge Rozeira. 2013. PH 2-A dermoscopic image database for research and benchmarking. In *Proceedings of the 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 5437–5440.

[18] Manoranjan Mohanty, Muhammad Rizwan Asghar, and Giovanni Russello. 2016. $2DCrypt$: Image scaling and cropping in encrypted domains. *IEEE Transactions on Information Forensics and Security* 11, 11 (2016), 2542–2555.

[19] Nathan Moroney. 2000. Local color correction using non-linear masking. In *Proceedings of the Color and Imaging Conference*. Society for Imaging Science and Technology, 108–111.

[20] Amitava Nag, Jyoti Prakash Singh, and Amit Kumar Singh. 2019. An efficient Boolean based multi-secret image sharing scheme. *Multimedia Tools and Applications* (2019), 1–25.

[21] J. Jesu Vedha Nayahi and V. Kavitha. 2017. Privacy and utility preserving data clustering for data anonymization and distribution on Hadoop. *Future Generation Computer Systems* 74 (2017), 393–408.

[22] Lina Ni, Chao Li, Xiao Wang, Honglu Jiang, and Jiguo Yu. 2018. DP-MCDBSCAN: Differential privacy preserving multi-core DBSCAN clustering for network user data. *IEEE Access* 6 (2018), 21053–21063.

[23] Şaban Öztürk and Umut Özkaya. 2020. Skin lesion segmentation with improved convolutional neural network. *Journal of Digital Imaging* (2020).

[24] Pascal Paillier. 1999. Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 223–238.

[25] Hongping Pang and Baocang Wang. 2020. Privacy-preserving association rule mining using homomorphic encryption in a multikey environment. *IEEE Systems Journal* (2020).

[26] Sankita Patel, Sweta Garasia, and Devesh Jinwala. 2012. An efficient approach for privacy preserving distributed K-means clustering based on shamir's secret sharing scheme. In *Proceedings of the IFIP International Conference on Trust Management*. Springer, 129–141.

[27] A. J. Paverd, Andrew Martin, and Ian Brown. 2014. Modelling and automatically analysing privacy properties for honest-but-curious adversaries. *University of Oxford, Tech. Rep* (2014).

[28] Nikolaos Polatidis, Christos K. Georgiadis, Elias Pimenidis, and Haralambos Mouratidis. 2017. Privacy-preserving collaborative recommendations based on random perturbations. *Expert Systems with Applications* 71 (2017), 18–25.

[29] Amitesh Singh Rajput and Balasubramanian Raman. 2018. Cloud based image color transfer and storage in encrypted domain. *Multimedia Tools and Applications* 77, 16 (2018), 21509–21537.

[30] Aqeel Sahi, David Lai, and Yan Li. 2016. Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. *Computers in Biology and Medicine* 78 (2016), 1–8.

[31] Adi Shamir. 1979. How to share a secret. *Commun. ACM* 22, 11 (1979), 612–613.

[32] Amit Kumar Singh. 2017. Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications* 76, 6 (2017), 8881–8900.

[33] Priyanka Singh, Balasubramanian Raman, and Nishant Agarwal. 2018. Toward encrypted video tampering detection and localization based on POB number system over cloud. *IEEE Transactions on Circuits and Systems for Video Technology* 28(9), 9 (2018), 2116–2130.

[34] A. Sreekumar and S. B. Sundar. 2009. An efficient secret sharing scheme for n out of n scheme using pob-number system. In *Proc. Hack.* 33.

[35] N. Z. Tajeddin and B. M. Asl. 2016. A general algorithm for automatic lesion segmentation in dermoscopy images. In *Proceedings of the 23rd Iranian Conference on Biomedical Engineering.* 134–139.

[36] Philipp Tschandl, Christoph Sinz, and Harald Kittler. 2019. Domain-specific classification-pretrained fully convolutional network encoders for skin lesion segmentation. *Computers in Biology and Medicine* 104 (2019), 111–116.

[37] Kai Xing, Chunqiang Hu, Jiguo Yu, Xiuzhen Cheng, and Fengjuan Zhang. 2017. Mutual privacy preserving $k$-means clustering in social participatory sensing. *IEEE Transactions on Industrial Informatics* 13, 4 (2017), 2066–2076.

[38] Ji-Jiang Yang, Jian-Qiang Li, and Yu Niu. 2015. A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems* 43 (2015), 74–86.

[39] L. Yu, H. Chen, Q. Dou, J. Qin, and P. Heng. 2017. Automated melanoma recognition in dermoscopy images via very deep residual networks. *IEEE Transactions on Medical Imaging* 36, 4 (2017), 994–1004.

[40] Y. Yuan, M. Chao, and Y. Lo. 2017. Automatic skin lesion segmentation using deep fully convolutional networks with Jaccard distance. *IEEE Transactions on Medical Imaging* 36, 9 (2017), 1876–1886.

[41] Yading Yuan and Yeh-Chi Lo. 2017. Improving dermoscopic image segmentation with enhanced convolutional-deconvolutional networks. *IEEE Journal of Biomedical and Health Informatics* (2017).

[42] Jiale Zhang, Yanchao Zhao, Jie Wu, and Bing Chen. 2020. LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT. *IEEE Internet of Things Journal* 7, 5 (2020), 4016–4027.

[43] Qingchen Zhang, Laurence T. Yang, Zhikui Chen, and Peng Li. 2017. PPHOPCM: Privacy-preserving high-order possibilistic c-means algorithm for big data clustering with cloud computing. *IEEE Transactions on Big Data,* doi=10.1109/TBDATA.2017.2701816 (2017).

[44] Xuyun Zhang, Laurence T. Yang, Chang Liu, and Jinjun Chen. 2014. A scalable two-phase top-down specialization approach for data anonymization using mapreduce on cloud. *IEEE Transactions on Parallel and Distributed Systems* 25, 2 (2014), 363–373.

[45] Zhili Zhou, Yunlong Wang, Q. M. Jonathan Wu, Ching-Nung Yang, and Xingming Sun. 2016. Effective and efficient global context verification for image copy detection. *IEEE Transactions on Information Forensics and Security* 12, 1 (2016), 48–63.

Received June 2020; revised October 2020; accepted October 2020