Crypt-OR: A privacy-preserving system for exemplar-based object-removal over the cloud

Vishesh Kumar Tanwar^{a,c,*}, Balasubramanian Raman^{b,c}, Rama Bhargava^{a,c}

^a*Department of Mathematics*

^b*Machine Vision Lab, Department of Computer Science & Engineering*

^c*Indian Institute of Technology Roorkee, INDIA*

Abstract

Object removal is a technique for removing the undesired object(s) and then fill-in the empty region(s) in an image such that the modified image is visually plausible. The existing algorithms are unable to provide promising results when the region to be removed - has varying textured-neighborhood, is small in size and the depth of the image and, is of specific geometric shapes such as triangle and rectangle. In this paper, we proposed a new algorithm by incorporating the merits of partial differential equations (PDEs) and exemplar-based schemes to address these challenges. The data term, which measures the continuity of isophotes in exemplar-based methods, is modified by incorporating a regularizer term and partial derivatives up to second order of the input image. This regularizer enhances the strength of isophotes striking the boundary and boosts the information propagation in an unbiased manner, in terms of pixel intensity values. Additionally, the low-cost, agility, and accessing flexibility benefits of cloud services have attracted user's attention today. Besides, users are concerned about utilizing them for their data, as they are supported by untrusted third parties. Addressing these privacy concerns for object-removal in an image over the cloud server, we extended and modified our algorithm to make it compatible for (T, N) -threshold Shamir secret sharing scheme (SSS). This

* Corresponding author

Email addresses: vtanwar@ma.iitr.ac.in (Vishesh Kumar Tanwar), bala@cs.iitr.ac.in (Balasubramanian Raman), rama.bhargava@ma.iitr.ac.in (Rama Bhargava)

privacy-preserving system is an end-to-end system for object-removal in the ED over the cloud server namely *Crypt-OR*. *Crypt-OR* is evaluated by removing synthetically imposed objects in real-images. Further, *Crypt-OR* has proved to be secure under various pixel-based cryptographic attacks such as frequency-known attack and pixel-correlation attack.

Keywords: Cloud computing, Image inpainting, Visual cryptography, Encrypted domain, Shamir secret sharing scheme

1. Introduction

Over the last decade, numerous images/videos algorithms for object recognition, classification, pose estimation and, semantic segmentation have been proposed Guo et al. (2016); Voulodimos et al. (2018). Besides their high perfor-

5 mances, these schemes are time-consuming and require high-configuration computing resources such as GPUs. To facilitate users, the Cloud Service Providers, hereafter abbreviated as CSP, are providing services such as Platform-as-a-service (PaaS), Infrastructure-as-a-Service (IaaS), and Software-as-a-service (SaaS) for accomplishing their tasks. Azure Machine Learning¹, Google Prediction

10 API², Amazon Rekognition³ are few instances. In SaaS, users have to share their private data, which may contain confidential and sensitive information, with CSP to utilize the services. Besides the excellent benefits given by CSPs, users are always concerned about data breaching. The consternation of data storage to CSP has been resolved with Advanced Encryption Standards (AES),

15 as no data, in particular images, can be revealed from their encrypted version Kaur & Kumar (2018), even with the infinite computational resources. In contrast, processing an encrypted image to achieve the same results as that of plain (non-encrypted) image constitutes a challenging problem, because encryption schemes distort pixels inter-correlation and *trichotomy law* in pixel-intensities.

¹ <https://azure.microsoft.com/en-in/services/machine-learning/>

² <https://cloud.google.com/ai-platform> ³ <https://aws.amazon.com/rekognition/>

20 *1.1. Privacy-preserving image processing*

Recently, researchers have presented several image/video processing models to perform different tasks in the ED. Lathey et al. Lathey et al. (2013); Lathey & Atrey (2015) have proposed a technique for privacy-preserving image enhancement such as noise removal, smoothing, and sharpening, in the ED. The image is secured through (N, T) -threshold Secret Sharing Scheme (SSS) Shamir
25 (1979). Shamir’s SSS is a homomorphic encryption scheme that partitions a secret s into N shares and requires at-least T shares to reconstruct s losslessly. Individually, each share appears random and contains zero information making the scheme secure. On reconstructing with less than T -shares, the resultant
30 value is equivalent to zero information. Similarly, Mohanty et al. Mohanty et al. (2013) and Tanwar et al. Tanwar et al. (2018a) have presented schemes for privacy-preserving image resizing and cropping in ED over the cloud. The ramp SSS is utilized to secure the user’s image from an adversary and interpolation technique over known intensity values to compute unknown pixel-intensities
35 in ED. A scheme for extracting and locating face regions in ED is proposed by Yan and Kankanhali Yan & Kankanhalli (2015). They secured the image information using coefficients of discrete cosine transform. Rahulamathavan et al. Rahulamathavan et al. (2013) presented a facial expression recognition system in an encrypted image, through Paillier cryptosystem, using local fisher discriminant analysis. Sayed et al. SaghaianNejadEsfahani et al. (2012) proposed an information-theoretical wavelet denoising model based on interactive protocols of SSS. They utilized the additive and scalar-multiplicative homomorphisms of Shamir’s SSS for basic filtering and thresholding operations that occur during the denoising process. Alberto et al. Pedrouzo-Ulloa et al. (2016) presented
45 a secure image denoising model using ring learning with errors, a lattice-based cryptosystem, which is fully non-interactive in comparison to SaghaianNejadEsfahani et al. (2012).

Hsu et al. Hsu et al. (2012) proposed a model for extracting SIFT features in ED using the Paillier cryptosystem. Chu et al. Chu et al. (2013) presented
50 a real-time object detection model for video surveillance. The scheme trans-

formed each frame into multiple blocks, and then each block is multiplied by a random matrix. Further, the Gaussian mixture model is used for detecting a moving object(s). The encryption is performed by matrix permutation and color flipping. However, using the same encryption key for the whole process
55 in video surveillance increases the rate of collision attacks. Additionally, Chu et al.’s model is based on each pixel-level operation, which highly increases the computational complexity. In Orlandi et al. (2007), an interactive protocol between the model and the data owners for evaluating the activation functions in the neural network is presented using Homomorphic Encryption (HE). Xie et al. Xie et al. (2014) and Gilad et al. Gilad-Bachrach et al. (2016) proposed
60 privacy-preserving image classification using Fully Homomorphic Encryption (FHE) Rivest et al. (1978) scheme. The utilization of FHE algorithms exponentially increases the computation overhead, making them impractical for real applications.

65 1.2. Image inpainting

It is a process of modifying images such that an unseen observer is unable to differentiate the original and inpainted image. In the ancient period, it was practiced by art-workers for restoring their images to make them “up to date”. The objective of image inpainting is to fill the deteriorated region in an image
70 to make them more visually appealing.

Diffusion-based inpainting techniques utilize the propagating-structure of heat flow through diffusion Partial Differential Equations (PDEs), to propagate the local information to the region to be inpainted Ω . An iterative mathematical formulating the technique performed by the professional inpaint art-workers
75 was presented by Bertalmio et al. Bertalmio et al. (2000). The formulation leverage the isophotes-prolongation technique of Masnou and Morel Masnou & Morel (1998) arriving at the boundary of Ω . The isophotes are propagated in the inward direction in such that they do not cross themselves and generate undesired results. The authors tested their scheme to remove the scratches and
80 overlaid-texts in an image. Following, numerous amount of inpainting models

incorporating the variants of linear and non-linear isotropic/anisotropic diffusion equations Bertalmio et al. (2001); Peter et al. (2016) have been proposed. These schemes are capable of completing the curves and small-sized objects; however, they generate smoothing/blurring effects for large and textured regions.

85 These perplexities have been addressed in Criminisi et al. (2004); Wang et al. (2013); Xiang et al. (2019) using exemplar-based texture synthesis approach presented by Efros and Leung Efros & Leung (1999). These schemes scan the source region Φ to obtain the best-exemplar patches for the region Ω , determined by similarity metric. Then, these patches are copied in the respective positions
 90 in Ω . Because of the “No Free Lunch Theorem”, these schemes are found to output unconnected edges. To connect these edges, researchers have combined theories of the categories mentioned above and proposed hierarchical schemes which improve perceptual and visual plausible Drori et al. (2003); Arias et al. (2011). Recently, the data-driven and parameter learning-based schemes using
 95 Convolutional Neural Networks (CNNs) have been proposed Nazeri et al. (2019); Yu et al. (2018). Nazeri et al. Nazeri et al. (2019) scheme is a two-stage approach, i.e., structure prediction and image completion. Both of these steps utilize the adversarial model, a variant of deep learning models. The scheme hallucinates the edges of the regions to be inpaint and then utilizes these edges
 100 to fill-in the region for image completion. Yu et al. Yu et al. (2018) scheme is a generative model, based upon feed-forward convolutional neural networks (CNNs), for synthesizing image structure and surrounding image features. Their model is evaluated to fill-in multiple only square-shaped holes irrespective of size and location. However, these learning models require a huge amount of training
 105 data and computational resources for significant results. For a detailed overview of image inpainting, ref. Guillemot & Le Meur (2013).

Nowadays, CSPs are providing inpainting SaaS such as Webpaint¹ and Photoscissors². They require the user’s image in a plausible visual form, which increases the concerns towards the protection of image information. Moreover,

¹ <https://www.webinpaint.com/> ² <https://online.photoscissors.com/>

110 the existing inpainting techniques cannot be directly implemented in ED due to their dependency on neighboring pixels, and distortion occurred through encryption techniques.

In the context of image inpainting, Yan et al. (2018) proposed a partial secret image sharing scheme for hiding the desired region of the image rather than the whole image. Their technique fills the target region by using the 115 inpainting technique in PD, which reveals the information of non-inpainting or source region while inpainting is performed over the cloud. We address above concerns and propose *Crypt-OR*, a privacy-preserving end-to-end system for removing object(s), specified by the user, in ED.

120 1.3. Contributions

The key contributions of the paper are as follows -

1. A new image inpainting scheme for object-removal is proposed. The data term, which measures the continuity of isophotes in exemplar-based methods, is introduced by integrating a regularizer and partial derivatives up to 125 second order of the input image. These derivatives improve the propagation efficiency of texture and structural information from the source region to the target region in the isophotes directions. The priority function is defined as the linear function of confidence and data terms.
2. The proposed scheme is extended to develop a privacy-preserving object-removal model, *Crypt-OR*, for removing pre-defined undesired object(s) 130 and fill-up the scratches occurred in images in the ED over the cloud infrastructures. The model encourages CSP to search the best-exemplar corresponding to the query patch in ED. The governing equations of inpainting in PD are transformed to make them compatible with the homomorphic properties of Shamir's SSS. 135
3. The scheme has proved to be secure under various cryptographic attacks such as *Frequency-known attack* and *Pixels-correlation attack*. *Crypt-OR* does not depend upon the topological shape of the region to be inpainted.

Figure 1: A general framework of exemplar-based image inpainting. (a) Original image I with region to be inpaint Ω and source region Φ . (b) It represents the possible patch candidates (in red) corresponding to the patch patch with center p (in green), (c) inpainted image.

The proposed model is evaluated over various images with the different region(s). The PSNR, SSIM, ASVS, and DN measures are reported, which are found to be very close to that of the existing scheme in PD.

4. To best of our knowledge, *Crypt-OR* is the first move towards removing objects in a given image in the ED using a search-copy-paste approach incorporating the cloud infrastructure(s).

Organization: Section 3 is devoted to describing Shamir’s SSS and the fundamentals of the exemplar-based scheme. The proposed framework for *Crypt-OR* is defined in Section 4 and, security analysis in Section 5. The qualitative and quantitative analysis of the proposed scheme are provided in Section 6, followed by discussion and analysis in Section 7. Finally, Section 8 concludes the paper.

2. Related Work

Over the recent decades, researchers have proposed various privacy preserving schemes for processing multimedia Bost et al. (2015); Lathey et al. (2013);

Jha et al. (2005); Orlandi et al. (2007). We discuss a glimpse of privacy preserving models for various image processing and other Machine Learning (ML) tasks.
 155 A detailed survey for preserving visual data was presented by Padilla-López et al. Padilla-López et al. (2015).

2.1. Privacy-preserving processing

The existing privacy preserving systems address the tasks of enhancement and feature extraction Lathey et al. (2013); Lathey & Atrey (2015); Tanwar et al.
 160 (2018b) over the ED. The scheme proposed by Lathey et al. Lathey et al. (2013); Lathey & Atrey (2015) is efficient for noise removal, edge sharpening, unsharp masking and anti-aliasing from an image in ED. The image is secured through (N, K) -threshold Shamir Secret Sharing (SSS) scheme. Tanwar et al. Tanwar et al. (2018b) proposed a privacy preserving algorithm for image scaling over
 165 the cloud in which image is encrypted by ramp SSS. They utilized 2D-Bicubic interpolation to interpolate the new pixel intensity values over cloud shares. A novel scheme for extracting and locating face regions in ED is proposed by Yan and Kankanhali Yan & Kankanhalli (2015). The information of image is preserved using coefficients of discrete cosine transform. Rahulamathavan et al.
 170 Rahulamathavan et al. (2013) presented a facial expressions recognition system in ED using local fisher discriminant analysis. The input image is encrypted using Paillier cryptosystem.

2.2. Privacy-preserving clustering

Clustering is an unsupervised ML task, which aims to partition a group of
 175 D -dimensional data points into K different subgroups, formally known as clusters, based on similarity metric. Researchers have proposed privacy preserving models for performing clustering in ED for vertically Jha et al. (2005); ? and arbitrary ?? partitioned data. Zhang et al. ? proposed a possibilistic c-means algorithm for fuzzy clustering of FHE encrypted big data. Xing et al. Xing et al.
 180 (2017) proposed a two-stage protocol for privacy preserving k -means clustering based on Paillier cryptosystem over social networking big-data.

2.3. Privacy-preserving recognition

As discussed earlier, various models for accomplishing recognition tasks while preserving data privacy have been presented Ma et al. (2018); Yonetani et al. (2017); Xie et al. (2014); Gilad-Bachrach et al. (2016); Orlandi et al. (2007); Bost et al. (2015); Shokri & Shmatikov (2015).

Authors in Xie et al. (2014); Gilad-Bachrach et al. (2016) proposed FHE-based Rivest et al. (1978) classification schemes which provides results similar to plain domain. The utilization of FHE techniques exponentially increase the computation overhead making these schemes impractical. In Orlandi et al. (2007), an interactive protocol between the model and data owners for evaluating the activation functions in neural network is presented using Homomorphic Encryption (HE). Bost et al. (2015) proposed a scheme for Naive Bayes, Decision Trees and Hyperplane Decision classifiers. The authors combined FHE without bootstrapping, Quadratic Residuosity and Paillier cryptosystems for encrypting data. In comparison with existing schemes Xie et al. (2014); Gilad-Bachrach et al. (2016); Bost et al. (2015), *SecureDL* is more computation and communication efficient.

3. Preliminaries

3.1. Shamir SSS

The scheme proposed by Adi Shamir Shamir (1979) states that if a secret value s , is shared into N meaningless shares, then T or more shares are required for lossless reconstruction of s , where T and N are positive integers such that $T \leq N$. The shares of s are generated via a polynomial $g(x)$ of degree $(T - 1)$, defined as:

$$g(x) = (s + c_1x + c_2x^2 + \dots + c_{T-1}x^{(T-1)}) \bmod \Upsilon \quad (1)$$

where the coefficients $c_1, \dots, c_{T-1}$ are randomly chosen from a Galois field of prime order Υ , denoted as $\mathbb{GF}(\Upsilon)$ and $x \in [1, N]$ is an integer.

The reconstruction of s from its N shares say $\{S_1, S_2, \dots, S_N\}$ is accomplished using Lagrange's interpolation over more than $T - 1$ shares. Moreover, the Shamir's SSS has been proved to be a *correct* and *perfect*, in the sense that - (a) out of N shares, T or more shares can reconstruct the secret value losslessly, (b) the zero information will reveal if reconstruction is performed using less than T shares. Also, Shamir's SSS is homomorphic with respect to addition and scalar multiplication.

3.2. Exemplar-based technique - Fundamentals

Consider an image I , in which user aims to remove and fill-in the target region Ω , using the source region Φ , where $\Phi = I - \Omega$. The boundary between these regions is denoted by $\partial\Omega$, as depicted in Fig. 1(a). For pixel p , Ψ_p indicates a patch or window of size $w \times w$ centered at p , as presented in Fig. 1(a). The standard rule-of-thumb in exemplar-based inpainting consists three steps as follows:

3.2.1. Computing patch priorities

For pixel $p \in \partial\Omega$, the priority value $P(p)$ of patch Ψ_p is evaluated as a product of integral powers of confidence term $C(p)$ and a data term $D(p)$ as -

$$P(p) = [C(p)]^\alpha [D(p)]^\beta, \quad \alpha, \beta \in \mathbb{N}$$

$$C(p) = \frac{\sum_{q \in \Psi_p \cap (I - \Omega)} C(q)}{\#(\Psi_p)} \quad \text{and} \quad D(p) = \frac{|\Delta I_p^\perp \cdot \vec{n}_p|}{\Gamma} \quad (2)$$

where $\#(\Psi_p)$ and Γ indicate the number of pixels in Ψ_p and normalization factor respectively. The term $C(p)$ is considered as the amount of reliable and meaningful information surrounding the pixel p . The $D(p)$ term measures the continuity of isophotes in their direction and helps to improve the priority of patch along the isophotes direction. $D(p)$ is calculated as a vector product of intensity gradient in an orthogonal direction $\Delta I_p^\perp$ and the normalized vector $\vec{n}_p$, of the binary mask M depicting Φ and Ω only, as shown in Fig. 1(a).

3.2.2. Finding optimal patch

Among all patches centered on $\delta\Omega$ i.e., $\{\Psi_{p_1}, \Psi_{p_2}, \dots, \Psi_{p_L}\}$, the patch Ψ_p having maximum priority value $P(p)$ corresponding to pixel p is considered. Then, the technique searches a patch say $\Psi_{q'}$, in Φ having maximum similarity measure with Ψ_p as shown in Fig. 1(b).

3.2.3. Propagation of source information

Once the optimal patch $\Psi_{q'}$ is obtained, the unknown pixel values in Ψ_p are replaced with the corresponding values in $\Psi_{q'}$. It can easily be observed in Fig. 1(c). Finally, confidence values of unknown pixels are updated through

$$C(p) = C(p') \quad \forall \quad p \in \Psi_{q'} \cap \Omega \quad (3)$$

4. Proposed methodology

The proposed *Crypt-OR* removes the undesired object(s) and fills in the scratches in an image using an exemplar-based inpainting approach. In contrast with the classical data term and priority function, an *Improved priority function*, denoted as $P_{imp}(p)$, and *Regularized data term*, denoted by $D_{reg}(p)$ respectively at pixel p are introduced. As discussed earlier, the schemes of PD cannot be directly applied to encrypted images. Therefore, the mathematical equations are modified depending upon the homomorphic operations, addition and scalar multiplication, of Shamir's SSS. Further, a protocol between the user and CSP is provided to accomplish the inpainting task at cloud servers.

In *Crypt-OR*, two entities are involved: (i) User: who aims to outsource his image I for removing the undesired region, denoted by Ω , in a secure manner and, (ii) CSP: who is "honest-but-curious" and accomplishes the task of inpainting in the encrypted share over the cloud server. CSP maintains the confidentiality, integrity and uniqueness of the share content provided by the user. The functions to be used are -

- MaskForm(): The input of this function is an image I in which the region Ω is highlighted with a specific color say red. The highlighting can easily be performed using Microsoft paint. It outputs a binary mask M indicating Ω and the source region Φ .
- DeriVal(): This function inputs I and M , thereby computing their partial derivatives upto second-order with respect to spatial variables.
- PatchEval(): It takes the priority values $\{P(p_z)\}_{z=1}^Z$ for pixels $\{p_z\}_{z=1}^Z$ in $\delta\Omega$ and outputs the most suitable patch.
- UpdateVal(): It updates the regularized data term $D_{reg}(p)$ and confidence value $C(p)$ for pixel p in Ω .
- ShareGen(): It takes image I and the parameters (N, T) of Shamir's SSS as input and, generates N obfuscated shares say $S_1, S_2, \dots, S_N$.

4.1. Regularized data term

The proposed data term, $D_{reg}(p)$, is defined as -

$$D_{reg}(p) = ||D_1(p)|| + ||D_2(p)|| + ||D_3(p)|| + \lambda\sqrt{||\mathcal{R}||} \quad (4)$$

the term $\sqrt{||\mathcal{R}||}$ indicates the introduced regularizer, and

$$D_1(p) = \left[\frac{-\partial I(p)}{\partial y}, \frac{\partial I(p)}{\partial x} \right] \odot \left[\frac{\partial M(p)}{\partial x}, \frac{\partial M(p)}{\partial y} \right] \quad (5)$$

$$D_2(p) = \left[\frac{-\partial^2 I(p)}{\partial y^2}, \frac{\partial^2 I(p)}{\partial x^2} \right] \odot \left[\frac{\partial^2 M(p)}{\partial x^2}, \frac{\partial^2 M(p)}{\partial y^2} \right] \quad (6)$$

$$D_3(p) = \left[\frac{-\partial^2 I(p)}{\partial x \partial y}, \frac{\partial^2 I(p)}{\partial y \partial x} \right] \odot \left[\frac{\partial^2 M(p)}{\partial y \partial x}, \frac{\partial^2 M(p)}{\partial x \partial y} \right] \odot C \quad (7)$$

$$\mathcal{R} = [\lambda_1, \lambda_2] \odot \left[\left(\frac{\partial M(p)}{\partial x} \right)^2, \left(\frac{\partial M(p)}{\partial y} \right)^2 \right] \quad (8)$$

where, $C = [0.5, 0.5]$, λ is a constant, $\odot$ represents the Hadamard matrix product, $||\cdot||$ is a function which sums the entries of the input vector and $\frac{\partial L(p)}{\partial t}$ is rate of change of intensity values in $L \in \{I, M\}$ in spatial direction $t \in \{x, y\}$ at pixel p . Similarly, $\frac{\partial^2 L(p)}{\partial x^2}$ and $\frac{\partial^2 L(p)}{\partial y^2}$ represent the acceleration of intensity flow in horizontal and vertical direction respectively. The mixed derivative term $\frac{\partial^2 L(p)}{\partial x \partial y}$ depicts the rate of change of L in x -direction followed by y -direction. Intuitively, it shows the changes occurred in non-linear curves.

Each term presented in D_{reg} has different significance in propagating the information in isophotes direction. The term $D_1(p)$ computes the maximum orthogonal rate of change of intensity values in each spatial direction of I , towards the front-line of boundary $\partial\Omega$. It only incites to incorporate the linear structures for information propagation which may fail to work in real-time images. $D_2(p)$ aims to evaluate the magnitude of maximum change in the neighborhood of p in vertical and both horizontal directions of the respective gradients. This term helps to find the direction of edges and sharp changes in I . The third term $D_3(p)$ motivates to evaluate the curves in the diagonal and cross-diagonal directions. It is important to realize that D_{reg} contains partial derivatives of second order which boosts data term and hence, improved priority function, $P_{imp}(p)$, to detect non-linear curves in I . Finally, the regularizer term boosts the information propagation in an unbiased manner, in terms of pixel intensities.

4.2. Improved priority function

In previous works, priority function for pixel p is given as the product of integral powers of $D(p)$ and $C(p)$ such as in Eq. 2. Experimentally, it is observed that $C(p)$ is inversely proportional to the exponential power of iteration number and hence, approaches to zero for large number of iterations Cheng et al. (2005). This makes the priority value $P(p)$, as defined in Eq. 2, to tend zero without considering the $D(p)$ value and thus, calculation of $P(p)$ becomes meaningless. Due to this, the scheme propagates the undesirable structure and texture information in the target region. Also, each pixel-intensity value is highly inter-correlated with its neighboring pixels and most likely information

Figure 2: The pictorial representation of *Crypt-OR*.

lies in the isophotes direction. Additionally, the neighboring information of the target patch for the continuous and meaningful propagation of structure and texture information is considered. In our proposed work, the improved priority
 305 function for a pixel p , denoted by $P_{imp}(p)$, is defined as a linear operator of $C(p)$ and $D_{reg}(p)$ as defined in Eq. 2 and Eq. 4 respectively. The mathematical equation is:

$$\begin{aligned}
 P_{imp}(p) &= [\alpha_1 \times C(p) + \beta_1] + [\alpha_2 \times D_{reg}(p) + \beta_2] \\
 \text{or} \quad &= \alpha_1 \times C(p) + \alpha_2 \times D_{reg}(p) + (\beta_1 + \beta_2) \\
 \text{or} \quad &= \alpha_1 \times C(p) + \alpha_2 \times D_{reg}(p) + \beta_3
 \end{aligned} \tag{9}$$

where $\beta_3 = (\beta_1 + \beta_2)$ and α_i, β_i are arbitrary hyper-parameters whose values are evaluated through experiments. The value of hyper-parameters are not equal
 310 which leads to a non-uniform contribution by each of $C(p)$ and $D_{reg}(p)$ to $P(p)$. Moreover, β_3 helps to maintain the existence of $P(p)$ with non-zero value when number of iterations increase.

4.3. Step-by-step description

In this section, we present the protocol of *Crypt-OR* which clearly explains
 315 the contribution of each entity - user and CSP. Assume an $M \times N$ -dimensional
 gray-scale image I in which region Ω is aimed to remove and fill-in. Note that the
 inpainting for true-color RGB image can be accomplished by performing each
 operation over each color channel independently. The pictorial explanation of
Crypt-OR is presented in Fig. 2. The outline of the proposed protocol is as
 320 follows -

Step 1: The region Ω in I is based upon user's requirement, therefore, it has
 be provided by the user, partitioning Ω and source region $\Phi = I - \Omega$. A binary
 mask M is generated utilizing the function `MaskForm()`. The partial derivatives
 of I upto second-order with respect to its spatial variables

are computed using function `DeriVal()`. Since, I is a 2-D discrete signal, so,
 these derivatives are approximated using finite difference methods. For instance,
 the approximations of $\frac{\partial I(p)}{\partial x}$, $\frac{\partial^2 I(p)}{\partial x^2}$, and $\frac{\partial^2 I(p)}{\partial x \partial y}$ at $p = (x, y)$, are as follows -

$$\frac{\partial I(p)}{\partial x} \approx \frac{I_{x+1,y} - I_{x-1,y}}{2} \quad (10)$$

325

$$\frac{\partial^2 I(p)}{\partial x \partial y} \approx \frac{I_{x-2,y} - 2 \times I_{x,y} + I_{x+2,y}}{4} \quad (11)$$

$$\frac{\partial^2 I(p)}{\partial x^2} \approx \frac{I_{x-1,y-1} - I_{x+1,y-1} - I_{x-1,y+1} + I_{x+1,y+1}}{4} \quad (12)$$

where $I_{x,y}$ indicates intensity value of I at position (x, y) . Shamir's SSS is
 not homomorphic in multiplication and division operations, so, Eqs. 10 - 12
 will not provide same results as obtained in PD, when performed in ED. The
 330 shares are generated using modulo operation with prime Υ as defined in Eq. 1.
 Therefore, the above equations are modified as -

$$\frac{\partial I(p)}{\partial x} \approx \text{mod}[(I_{x-1,y} - I_{x+1,y}) + \Upsilon, \Upsilon] \quad (13)$$

$$\frac{\partial^2 I(p)}{\partial x \partial y} \approx \text{mod}[(I_{x-2,y} - 2 \times I_{x,y} + I_{x+2,y}) + \Upsilon, \Upsilon] \quad (14)$$

Similarly, other derivatives can be approximated with modulo operation. The square root contained in regularizer in Eq. 8 is approximated by *Taylor series* upto first order. Further, the confidence and data values for each pixel of I are initialized randomly using `ConfVal()` and `DataVal()` respectively.

Step 2: Here, user computes the partial derivatives of mask M upto second order using `DeriVal()`. It can be observed that these derivative values of M are zero inside the regions Ω and Φ , albeit, non-zero at the boundary $\partial\Omega$. Moving ahead, the priority values for each $p \in \partial\Omega$, is calculated using Eq. 9, under *modulo* operation. A pixel p having maximum priority value $P(p)$ is considered to start with and the corresponding patch Ψ_p of window size $w \times w$. Then, user operates `ShareGen()` to generate N shares say $\{S_1, S_2, \dots, S_N\}$ of I with prime Υ . It is observed that each share S_t depends upon random numbers c_j 's (Eq. 1), therefore, intensity values in Ψ_p changes accordingly. Let $\Psi_{p^t}^{Enc}$ denotes the patch Ψ_p in share S_t . Note that $\Psi_{p^t}^{Enc}$ varies with Ψ in terms of intensity values only, although, positions will unchanged. Now, the share S_t along with the patch $\Psi_{p^t}^{Enc}$ will be transmitted to CSP C_t , for $t = 1, 2, \dots, N$.

Step 3: After successfully receiving share S_t and $\Psi_{p^t}^{Enc}$, CSP C_t searches the best possible encrypted patch say $\Psi_{q^t}^{Enc}$ similar to $\Psi_{p^t}^{Enc}$. The searching is accomplished by defining a difference measure $G()$ between $\Psi_{p^t}^{Enc}$ and $\Psi_{q^t}^{Enc}$, for some l , in S_t as follows -

$$G_l = 2 \times Err_l + \Upsilon + (p - 1) \quad (15)$$

$$\text{where, } Err_l = \sum_{k=1}^{w^2} [\Psi_{q^t}^{Enc}(k) - \Psi_{p^t}^{Enc}(k)]$$

Note that $\Psi_{q^t}^{Enc}$ is of dimension $w \times w$ contained in Φ^{Enc} , source region in S_t

corresponding to the source region Φ of I . A patch having least difference value is considered as the best-exemplar $\Psi_{q^t}^{Enc}$ corresponding to $\Psi_{p^t}^{Enc}$ in S_t . Then,

335 C_t transmits back the obtained patch to user.

Step 4: User re-collect all N encrypted best-exemplar patches $\left\{\Psi_{q^l}^{Enc}\right\}_{l=1}^N$ corresponding to $\left\{\Psi_{q^l}^{Enc}\right\}_{l=1}^N$ obtained from N CSPs. Then, each encrypted patch $\Psi_{q^l}^{Enc}$ is decrypted to a patch in PD say Ψ_{q^l} . It can be clearly concluded that for $t_1 \neq t_2$, $\Psi_{q^{t_1}}$ may be different from $\Psi_{q^{t_2}}$. Therefore, the most suitable patch Ψ_q with respect to Ψ_p is procured by computing structural similarity value between each Ψ_{q^l} and Ψ_p . The patch having maximum similarity value is assumed to be best-exemplar Ψ_q . The unknown pixels of Ψ_p in Ω are replaced with the corresponding values of Ψ_q . As defined in Section 3.2, the data term $D_{reg}(p)$ and confidence values $C(p)$ are updated with the corresponding $C(p)$ and $D_{reg}(p)$ values of Ψ_p .

Step 5: Repeat Step 2 to Step 5 until the intensity values of all the pixels in Ω are obtained.

5. Security analysis

Here, the security analysis of *Crypt-OR* from an adversary is evaluated through standard image encryption tests Cao et al. (2018).

5.1. Frequency-known attack

In this attack, an adversary is given the frequencies of each pixel intensity value, known as frequency histogram, of an encrypted image (I_{Enc}), but not of the corresponding image I in PD. An adversary manages to extract the frequency histogram of I for given frequency histogram of I_{Enc} . The histogram of an image features the contrast, brightness and saturation effects of the contents. The attack demonstrates the change in diffusion and confusion characteristics of I_{Enc} in comparison with I . It is assumed that adversary has infinite amount of time and computational resources. In order to secure information in I from the adversary, frequency histogram of I_{Enc} must be significantly different from I and uniform as much as possible.

We consider the *Lena* image in RGB color-space, I , of dimension 256×256 and its respective red, green and blue channels histograms as depicted in Fig.

Figure 3: Histogram analysis of *Lena* RGB-image in PD and its encrypted shares.

3(a). The encrypted shares I_{S_1} and I_{S_2} of I under modulo $\Upsilon = 251$ are depicted
 365 in Fig. 3(b) and Fig. 3(c) respectively. It can be observed that histogram of

Figure 4: Histogram analysis of z-black image in PD and its encrypted shares.

each channel in PD contains multiple valley-like regions and pixel intensities lie in the range $[30, 255]$ (zoom-in horizontal axis). In contrast, the histograms of shares are different than that of secret image and almost uniform. They ranges nearly equal in interval $[0, 251]$ (zoom-in horizontal axis), which means that the pixels information is uniformly distributive over the whole range. Thus, CSPs can extract approximately zero information of user's secret image.

Figure 5: Histogram analysis of white image in PD and its encrypted shares.

Moreover, we perform encryption experiments for an image whose all pixel intensity values are equal i.e., constant image. An encryption scheme is assumed to be completely secure if its output does not depend upon the input values. In other words, the encrypted form of a constant image and real-time image say *Lena* are almost same. For this, a z-black and white images are considered as shown in Figs. 4 and 5. In each Figs. 4 and 5, (a) contains the original image and

the corresponding encrypted shares under modulo $\Upsilon = 251$. The corresponding histograms are presented in (b). Note that the histograms of black and white
380 images contain single spike to 0 and 255 respectively. However, their histograms are distributed uniformly over the range $[0, 251]$, proving the complete security of image information.

5.2. Pixels-correlation attack

The correlation between neighboring pixels in an image I depicts a statistical
385 relevance Chen et al. (2004). High pixels-correlation indicates the high-visual quality of an image, which helps to extract meaningful information. To prevent the information poses by I from an adversary, the correlation value must be low for its encrypted shares, which we analyze for *Crypt-OR*.

5.2.1. Numerical values

390 The correlation of K neighboring pixels $\{(x_1, y_1), (x_2, y_2), \dots, (x_K, y_K)\}$ for a gray-scale image I , denoted by $corr$, is evaluated as follows -

$$corr(x, y) = \frac{cov(x, y)}{SD(x) \times SD(y)} \quad (16)$$

where SD and $cov(x, y)$ represent the standard deviation and covariance respectively. It lies in $[-1, 1]$, with “-1” and “1” indicate perfect negative and positive correlation respectively and, no relation when it approaches “0”.

395 For experiments, *Lena* image and its encrypted share, Ref. Fig. 3(a) and (b), are considered. The $corr$ values in each of diagonal, horizontal and, vertical directions using randomly selected 2000 adjacent pixel pairs of I are presented in Table 1. It is observed that correlation of I is more than 0.92, whereas, in *Crypt-OR* it falls close to 0. It indicates that the proposed scheme efficiently
400 breaks the pixels inter-correlation. Further, the $corr$ values in *Crypt-OR* are compared with Chong et al. Fu et al. (2012), Teng et al. Teng & Wang (2012) and, Tanwar et al. Tanwar et al. (2018b).

Table 1: Comparison of correlation coefficient with existing schemes.

Direction	Horizontal	Vertical	Diagonal
Secret Image	0.9404	0.9299	0.9257
Chong et al. Fu et al. (2012)	0.0088	-0.0087	0.0060
Teng et al. Teng & Wang (2012)	0.0242	-0.0194	0.0243
Tanwar et al. Tanwar et al. (2018b)	0.0106	0.0112	0.0087
<i>Crypto-OR</i>	0.0041	-0.0084	0.0052

5.2.2. Visual analysis

The high value of correlation coefficient (Eq. 16) indicate the compact relation between the pixel intensity values and vice-versa for low correlation value. This compactness can be observed in first column of Fig. 6. The correlation of *Lena* gray-scale image of dimension 256×256 in each of vertical, horizontal, diagonal and anti-diagonal direction are shown in first column of Fig. 6 (b), (c), (d) and (e) respectively. The corresponding correlation of encrypted image I_{Enc} of *Lena* image in each directions are presented in second column of fig. 6. It indicates that the encrypted scheme efficiently secures the user image information from an adversary.

5.3. Differential analysis

Shamir's SSS adds a random number with each pixel intensity before generating the respective shares with varying prime numbers. With different random numbers, the encrypted form of secret image I must change. The changes are observed using Unified Average Changing Intensity (UACI) and Number of Pixels Changing Rate (NPCR) Chen et al. (2004).

Consider two encrypted image E_1^I and E_2^I , obtained before and after changing one pixel intensity of an $M \times N$ -dimensional image I . Let $E_1^I(i, j)$ and

$E_2^I(i, j)$ denote the intensities at pixel $(i, j)^{th}$ -position in E_1^I and E_2^I respectively. Then, UACI and NPCR are calculated as follows -

$$\text{UACI} = \frac{1}{M \times N} \left[\sum_{j=1}^M \sum_{i=1}^N \frac{|E_1^I(j, i) - E_2^I(j, i)|}{255} \right] \times 100 \% \quad (17)$$

$$\text{NPCR} = \frac{1}{M \times N} \left[\sum_{j=1}^M \sum_{i=1}^N D(j, i) \right] \times 100 \% \quad (18)$$

where,

Figure 6: Comparison of correlation coefficient of (a) *Lena* image and its encrypted share in (b) horizontal, (c) vertical, (d) diagonal and, (e) anti-diagonal directions.

$$D(j, i) = \begin{cases} 1, & E_1^I(j, i) \neq E_2^I(j, i) \\ 0, & E_1^I(j, i) = E_2^I(j, i) \end{cases} \quad (19)$$

The higher values of NPCR and UACI depict the high efficiency of the encryption algorithm to resist image information from differential attacks. For experiments, two shares of *Lena* image (Ref. Fig. 3 (a)) and the modified image obtained by interchanging two-pixels in each color channel at the same position are generated. Due to the addition of a random number, the average of 10 simultaneous NPCR and UACI values are reported as **99.9520%** and **33.2711%** respectively. The values determine that *Crypt-OR* can adequately

resist differential attacks, and an eavesdropper cannot extract any information even after a modification in intensity values of the secret image.

6. Experiments

In this section, the perceptual and statistical results of *Crypt-OR* are presented. The secret image I is encrypted into four obfuscated shares say $\{S_1, S_2, S_3, S_4\}$ with $\Upsilon = 251$. The reconstruction of inpainted image, denoted by I_{inp} is accomplished by combining all four processed shares $\{S'_1, S'_2, S'_3, S'_4\}$. In view of *Crypt-OR*, the numerical results are evaluated corresponding to the reconstructed inpainted image I_{inp} with patch size as 5. Codes are implemented using MATLAB 2017b running on 64-bit Ubuntu 16.04 OS, over a Dell PC with Intel(R) core i7-3770, 3.40 GHz processor, 8 GB of RAM. The robustness of *Crypt-OR* is validated by removing synthetically imposed geometric shapes such as star-like structure, rectangle, triangle and circle on datasets of textures, foods, monuments, mountains, waterfalls and Paris street views (PSV) containing 200 images of each type.

6.1. Qualitative analysis

The perceptual results of the reconstructed inpainted images are analyzed in three scenarios - baseline model in which the data term does not contain regularizer (8), baseline model with the regularizer $\mathcal{R}$ (Eq.8) in PD and *Crypt-OR*. The inpainted images are compared in Fig. 7. It can be observed that the baseline model is unable to propagate the information from the source region to the target region in various scenarios such as the depth object(s), ambiguous background, and large region. In contrast, the incorporation of regularizer with the baseline model effectively addresses these concerns. The numerical comparison in PD is performed; the SSIM, PSNR, ASVS, and DN values (Section 6.2) with the original image are provided. Further, the significance of regularizer with varying scenarios can be observed in the supplementary material.

Further, *Crypto-OR* is compared with the existing image inpainting and object-removal schemes presented by - Criminisi et al. Criminisi et al. (2004)

Figure 7: Comparison of the inpainted images in PD without and with regularizer in the data term. (a) Original image, (b) Superimposed object(s) to be removed are given in red color, (c) Baseline model, and (d) Baseline model with regularizer. The lined box(es) at the top/bottom of the image indicate the zoom-in portion of the dashed bounding-box(es). The impact of the regularizer can easily be observed in the lined-box(es) in (c) and (d), along with (a).

460 with patch size as 5 and, deep learning schemes of Nazeri et al. Nazeri et al.
 (2019) and Yu et al. Yu et al. (2018). The testing codes corresponding to inpaint
 model⁴ presented by Nazeri et al. (2019) and pre-trained adversarial model⁵ over
 Places2 dataset of Yu et al. (2018) are considered. The presented results are
 obtained without fine-tuning as authors have trained with regular and irregular
 465 patches provided by Liu et al. (2018). the results are depicted in Figs. 8 - 9.
 In each figure, the first row represents the original image with imposed red-
 colored region (Ω), aimed to remove. Second, third, and fourth rows indicate
 the inpainted images obtained by Criminisi et al. (2004), Nazeri et al. (2019), Yu
 et al. (2018) and, *Crypt-OR* respectively. It can easily be observed that *Crypt-*
 470 *OR* significantly removes the specified region except for minor artifacts in some
 images. It is important to note that *Crypt-OR* searches the best-exemplar in
 the ED as compared to the techniques Criminisi et al. (2004) which searches
 in PD. The learning-based schemes Nazeri et al. (2019); Yu et al. (2018) utilize
 variants of deep neural networks and require a huge amount of training data
 475 and high-configuration computational resources. Also, these schemes are highly
 biased upon the features, obtained from pixels high inter-correlation, of input
 images and types of the region to be inpainted, which can be observed in Fig.
 13. In contrast, image features are obfuscated in ED, and these schemes have
 to train their model depending upon the region Ω and encryption scheme to be
 480 used. More inpainted images are provided in the supplementary material.

6.2. Quantitative analysis

Here, the comparison of quantitative results of *Crypt-OR* with the existing
 inpainting schemes are presented. Due to the utilization of random numbers,
 while generating shares, each experiment is performed 10-times and their aver-
 485 age values are reported.

⁴ <https://github.com/knazeri/edge-connect> ⁵ <https://github.com/JiahuiYu/generative.inpainting>

Figure 8: Comparison of *Crypt-OR* over texture and food images. (a) Original image - red indicates the undesired region(s), (b) Criminisi et al. (2004), (c) Nazeri et al. (2019), (d) Yu et al. (2018), and (e) *Crypt-OR*. The resulting difference in each scheme can be observed (top-to-down) by zoom-in the rectangle(s) region(s).

Figure 9: Comparison of *Crypt-OR* over monument and mountain images. (a) Original image - red indicates the undesired region(s), (b) Criminisi et al. Criminisi et al. (2004), (c) Nazeri et al. Nazeri et al. (2019), (d) Yu et al. Yu et al. (2018), and (e) *Crypt-OR*. The resulting difference in each scheme can be observed (top-to-down) by zoom-in the rectangle(s) region(s).

6.2.1. Peak Signal-to-Noise Ratio (PSNR)

The PSNR between inpainted image (I) and original image (J) is evaluated using the following equation:

$$PSNR = 2 \times 10 \times \log_{10}(255) - 10 \times \log_{10}(MSE) \quad (20)$$

where MSE is mean squared error between I and J .

490 The quality of the inpainted image increases with higher PSNR value, which is reported in Fig. 10. It can easily be observed that *Crypt-OR* outperforms Criminisi's model in all scenarios except mountains and close to Yu et al. and Nazir et al. models. The quality of an inpainted image obtained by *Crypt-OR* is close to the deep learning-based schemes in PD.

Figure 10: Comparison of PSNR values.

495 6.2.2. Structural SIMilarity (SSIM) index

The luminance, contrast and structural similarity Wu et al. (2013) between original image (I) and inpainted image (J) is compare by computing Mean SSIM

Figure 11: Comparison of SSIM values.

(MSSIM) index over N_w number of local windows is computed as:

$$MSSIM = \frac{1}{N_w} \sum_{k=1}^{N_w} \frac{(2\mu_I\mu_J + C_1) \times (2\sigma_{IJ} + C_2)}{(\mu_I^2 + \mu_J^2 + C_1) \times (\sigma_I^2 + \sigma_J^2 + C_2)} \quad (21)$$

where σ_k and μ_k are standard deviation and average intensity value of $k \in \{I, J\}$. σ_{IJ} denotes correlation of I and J and, C_l 's are stability constants. Further, I_k and J_k indicate the image patches for k_{th} window. It lies in the interval $[0, 1]$, where the value near to 0 shows low structural similarity and that of 1 represents high structural similarity between I and J .

The MSSIM values obtained between the original and inpainted images are depicted in Fig. 11. *Crypt-OR* outperforms Criminisi et al. (2004) in all scenarios and close to Nazari et al. (2019) and Yu et al. (2018).

6.2.3. Image inpainting quality measure

The most reliable and accurate method to measure an image quality is the human-rating, the ultimate users. This measure is laborious, time consuming, and requires a large number of observers. Thus, a non-reference saliency-based

inpainting metrics namely *Average Squared Visual Saliency* (ASVS) and *Degree of Noticeability* (DN) proposed in Ardis & Singhal (2009) are utilized.

These metrics compute the distortions in the inpainted image, which occurred due to the propagation of different colors, structures, and textures from the source region Φ , to Ω . ASVS computes the amount of noticeability of Ω , in comparison with the whole image I , whereas DN measures the distortions that occurred in the neighborhood of Ω , plus to distortions occurred inside Ω . The mathematical definition is as follows -

$$\begin{aligned}
 ASVS &= \frac{1}{||\Omega||} \sum_{p \in \Omega} |S'_M(p)|^2 \times 100 \\
 DN &= \frac{100}{||\Omega|| + ||\Phi||} \left(\sum_{p \in \Omega} |S'_M(p)|^2 + \sum_{p \in \Phi} E(S'_M, S_M) \right) \\
 E(S'_M, S_M) &= |S'_M(p) - S_M(p)|
 \end{aligned} \tag{22}$$

where, $S'_M(p)$ depicts the saliency map value of the inpainted pixel p inside Ω , in the inpainted image and $||\Omega||$ indicates the area of Ω . The lower values of ASVS and DN represent the high perceptual quality of the inpainted image.

The average ASVS and DN values obtained by *Crypt-OR* are found to be comparable, except in mountain images, with the existing schemes Criminisi et al. (2004), Nazeri et al. (2019) and Yu et al. (2018) as shown in Fig. 12.

It can be observed that ASVS and DN values for *Crypt-OR* are less than the Criminisi et al. (2004) and equivalent to Nazeri et al. (2019); Yu et al. (2018), even lesser for images of texture, waterfall and PSV. Howbeit, it is high for mountain database. Similarly, DN values of *Crypt-OR* coincides with that of existing schemes Criminisi et al. (2004); Nazeri et al. (2019); Yu et al. (2018). In view of “No Free Lunch” theorem, *Crypt-OR* under-performs a bit for mountain database when compared with Nazeri et al. (2019); Yu et al. (2018), however, outperforms than Criminisi et al. (2004). The further analysis and comparison of *Crypt-OR* in view of structural similarity index and PSNR values are presented in supplementary material.

(a)

(b)

Figure 12: Comparison of (a) ASVS and, (b) DN values.

535 7. Discussion

Here, the key outcomes of the proposed inpainting scheme are discussed by removing synthetically imposed shapes in grayscale images, as depicted in Fig. 13(a). It is observed that Criminisi’s model Criminisi et al. (2004) can maintain the edges in an image, but also generates undesired information, except in the third row, Fig. 13(b). Nazeri et al. Nazeri et al. (2019) are unable to remove the specified region as the existing model was not trained for these shapes. Also, the neighboring background of the region has very little information and edges which the scheme can hallucinate, followed by completing the region. The inpainted images of Nazeri’s model can be visualized in Fig. 13(c). Yu et al. Yu et al. (2018) model is a generative approach that synthesizes the image structure and surrounding image features. It can be observed in Fig. 13(d) that the scheme fails to generate desirable results. Due to the non-availability of rich image features in the source region. The major drawbacks of these deep learning models are that they need to fine-tune/train over the new dataset with specific constraints as these are highly dependent upon the pixels inter-correlations. Also, they require high configured computing resources and storage space.

In contrast, *Crypt-OR* is a single-image based scheme and outperforms the existing schemes as depicted in Fig. 13 (e). It is observed that the proposed *regularizer* in data term and *improved priority function* generalize the behavior of structure and texture propagation in isophotes direction for the arbitrary region(s) to be inpaint. However, it is unable to propagate the edges of the triangle-shaped image (last-row), zoomed-in the upper corner of the triangle in Fig. 13(e), which is considered as future work.

7.1. Performance analysis

The computational cost required to remove the desired object(s) followed by fill-in the empty space using *Crypt-OR* consists of three processes - (i) encrypting the image into N Shamir’s shares, (ii) performing *Crypt-OR* over each share S_k and, (iii) reconstruction of an inpainted image using T inpainted shares. The processes (i) and (iii) are performed by the user and (ii) by CSP C_k . The total

Figure 13: Comparison of *Crypt-OR* over various geometric shapes. (a) Original image - red indicates the region to be removed, (b) Criminisi et al. Criminisi et al. (2004), (c) Nazeri et al. Nazeri et al. (2019), (d) Yu et al. Yu et al. (2018), and (e) *Crypt-OR*. The effective results can be analyzed by zoom-in the inpainted region.

Table 2: Performance analysis of object-removal in PD.

Region Percentage	Baseline model		Baseline with regularizer	
	Min	Max	Min	Max
3 - 5 %	5.03	18.45	5.99	22.89
6 - 10 %	7.12	23.84	8.63	27.02
11 - 15 %	10.78	29.57	12.92	34.35

565 required-time for each process varies with the computational resources utilized
 by the user and CSP. For experimentation, we perform all three processes on
 our system, Ref. 6. The secret image of dimension 256×256 is shared into
 4 Shamir’s shares, which requires a time of 0.54 second. The decryption time
 using all 4 inpainted shares is 1.30 seconds. The inpainting time varies with the
 570 desired region-size and shape, as given in Table 2.

8. Conclusion and future work

In this paper, a novel and efficient image inpainting model leveraging the
 merits of partial differential equations (PDEs) and exemplar-based schemes is
 proposed. A regularizer is introduced with the data-term for computing the
 575 isophotes strength striking the boundary of the region. The scheme addresses
 the challenges of the small-sized object(s) in the depth of the image, varying
 textured-background, and objects(s) of specific geometric shapes such as trian-
 gle and rectangle. The scheme is further extended to perform in the ED over
 the cloud server as a SaaS. The secret image information is bifurcated into mul-
 580 tiple shares of Shamir’s SSS. The qualitative and quantitative results obtained
 by *Crypt-OR* indicate the robust propagation of texture features and structure
 information in comparison with the existing schemes. The perceptual examples
 demonstrate that our scheme can be used for various applications such as re-
 moval of unwanted/undesired object(s), data hiding, and privacy surveillance.
 585 As future work, the removal of various facial features in a personal image in the
 ED over cloud infrastructures can be considered.

Acknowledgment

This work is sponsored under grant: 21/12/2014(ii)EU-V, 2121440593 by University Grant Commission, INDIA.

- 590 Ardis, P. A., & Singhal, A. (2009). Visual salience metrics for image inpainting. In *Visual Communications and Image Processing* (p. 72571W). International Society for Optics and Photonics volume 7257. doi:10.1117/12.808942.
- Arias, P., Facciolo, G., Caselles, V., & Sapiro, G. (2011). A variational framework for exemplar-based image inpainting. *International Journal of Computer Vision*, 93, 319–347.
- 595 Bertalmio, M., Bertozzi, A. L., & Sapiro, G. (2001). Navier-stokes, fluid dynamics, and image and video inpainting. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (pp. I–I). IEEE volume 1. doi:10.1109/CVPR.2001.990497.
- 600 Bertalmio, M., Sapiro, G., Caselles, V., & Ballester, C. (2000). Image inpainting. In *The Annual Conference on Computer Graphics and Interactive Techniques* (pp. 417–424). ACM Press/Addison-Wesley Publishing Co. doi:10.1145/344779.344972.
- Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. (2015). Machine learning classification over encrypted data. In *NDSS*.
- 605 Cao, C., Sun, K., & Liu, W. (2018). A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map. *Signal Processing*, 143, 122–133.
- Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, 21, 749–761.
- 610 Cheng, W.-H., Hsieh, C.-W., Lin, S.-K., Wang, C.-W., & Wu, J.-L. (2005). Robust algorithm for exemplar-based image inpainting. In *Proceedings of International Conference on Computer Graphics, Imaging and Visualization* (pp. 64–69).

- Chu, K.-Y., Kuo, Y.-H., & Hsu, W. H. (2013). Real-time privacy-preserving
615 moving object detection in the cloud. In *Proceedings of the ACM International Conference on Multimedia* (pp. 597–600). ACM. doi:10.1145/2502081.2502157.
- Criminisi, A., Pérez, P., & Toyama, K. (2004). Region filling and object removal by exemplar-based image inpainting. *IEEE Transactions on Image*
620 *Processing*, 13, 1200–1212. doi:10.1109/TIP.2004.833105.
- Drori, I., Cohen-Or, D., & Yeshurun, H. (2003). Fragment-based image completion. In *ACM Transactions on graphics* (pp. 303–312). ACM volume 22.
- Efros, A. A., & Leung, T. K. (1999). Texture synthesis by non-parametric sampling. In *International Conference on Computer Vision* (pp. 1033–1038).
625 IEEE volume 2.
- Fu, C., Chen, J., Zou, H., Meng, W., Zhan, Y., & Yu, Y. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics Express*, 20, 2363–2378. doi:10.1364/OE.20.002363.
- Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., & Wernsing,
630 J. (2016). Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In *International Conference on Machine Learning* (pp. 201–210).
- Guillemot, C., & Le Meur, O. (2013). Image inpainting: Overview and recent advances. *Signal Processing Magazine*, 31, 127–144.
- 635 Guo, Y., Liu, Y., Oerlemans, A., Lao, S., Wu, S., & Lew, M. S. (2016). Deep learning for visual understanding: A review. *Neurocomputing*, 187, 27–48.
- Hsu, C.-Y., Lu, C.-S., & Pei, S.-C. (2012). Image feature extraction in encrypted domain with privacy-preserving sift. *IEEE Transactions on Image Processing*, 21, 4593–4607.

- 640 Jha, S., Kruger, L., & McDaniel, P. (2005). Privacy preserving clustering.
In *European Symposium on Research in Computer Security* (pp. 397–417).
Springer. doi:10.1007/11555827_23.
- Kaur, M., & Kumar, V. (2018). A comprehensive review on image encryption
techniques. *Archives of Computational Methods in Engineering*, (pp. 1–29).
- 645 Lathey, A., & Atrey, P. K. (2015). Image enhancement in encrypted domain
over cloud. *ACM Transactions on Multimedia Computing, Communications,
and Applications*, 11, 38.
- Lathey, A., Atrey, P. K., & Joshi, N. (2013). Homomorphic low pass filtering on
encrypted multimedia over cloud. In *International Conference on Semantic*
650 *Computing* (pp. 310–313). IEEE.
- Liu, G., Reda, F. A., Shih, K. J., Wang, T.-C., Tao, A., & Catanzaro, B. (2018).
Image inpainting for irregular holes using partial convolutions. In *Proceedings
of the European Conference on Computer Vision* (pp. 85–100).
- Ma, X., Zhang, F., Chen, X., & Shen, J. (2018). Privacy preserving multi-party
655 computation delegation for deep learning in cloud computing. *Information
Sciences*, 459, 103–116.
- Masnou, S., & Morel, J.-M. (1998). Level lines based disocclusion. In *Interna-
tional Conference on Image Processing* (pp. 259–263). IEEE.
- Mohanty, M., Ooi, W. T., & Atrey, P. K. (2013). Scale me, crop me,
660 knowme not: Supporting scaling and cropping in secret image sharing. In
IEEE International Conference on Multimedia and Expo (pp. 1–6). IEEE.
doi:10.1109/ICME.2013.6607567.
- Nazeri, K., Ng, E., Joseph, T., Qureshi, F., & Ebrahimi, M. (2019). Edgecon-
nect: Structure guided image inpainting using edge prediction. In *Proceedings*
665 *of the IEEE International Conference on Computer Vision Workshops*.

- Orlandi, C., Piva, A., & Barni, M. (2007). Oblivious neural network computing via homomorphic encryption. *EURASIP Journal on Information Security*, 2007, 037343.
- 670 Padilla-López, J. R., Chaaraoui, A. A., & Flórez-Revuelta, F. (2015). Visual privacy protection methods: A survey. *Expert Systems with Applications*, 42, 4177–4195.
- Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J. R., & Pérez-González, F. (2016). Image denoising in the encrypted domain. In *International Workshop on Information Forensics and Security* (pp. 1–6). IEEE. doi:10.1109/WIFS. 2016.7823916.
- 675 Peter, P., Hoffmann, S., Nedwed, F., Hoeltgen, L., & Weickert, J. (2016). Evaluating the true potential of diffusion-based inpainting in a compression context. *Signal Processing: Image Communication*, 46, 40–53.
- Rahulamathavan, Y., Phan, R. C.-W., Chambers, J. A., & Parish, D. J. (2013). Facial expression recognition in the encrypted domain based on local fisher discriminant analysis. *IEEE Transactions on Affective Computing*, 4, 83–92.
- 680 Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation*, 4, 169–180.
- SaghaianNejadEsfahani, S. M., Luo, Y., & Cheung, S.-c. S. (2012). Privacy protected image denoising with secret shares. In *IEEE International Conference on Image Processing* (pp. 253–256). IEEE. doi:10.1109/ICIP.2012.6466843.
- 685 Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22, 612–613. doi:10.1145/359168.359176.
- Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In *ACM SIGSAC Conference on Computer and Communications Security* (pp. 1310–1321). ACM.
- 690

- Tanwar, V. K., Rajput, A. S., Raman, B., & Bhargava, R. (2018a). Privacy preserving image scaling using 2d bicubic interpolation over the cloud. *International Conference on Systems, Man, and Cybernetics*, (pp. 2073–2078).
- 695 Tanwar, V. K., Rajput, A. S., Raman, B., & Bhargava, R. (2018b). Privacy preserving image scaling using 2d bicubic interpolation over the cloud. In *International Conference on Systems, Man, and Cybernetics* (pp. 2073–2078). IEEE.
- Teng, L., & Wang, X. (2012). A bit-level image encryption algorithm based on
700 spatiotemporal chaotic system and self-adaptive. *Optics Communications*, 285, 4048–4054. doi:10.1016/j.optcom.2012.06.004.
- Voulodimos, A., Doulamis, N., Doulamis, A., & Protopapadakis, E. (2018). Deep learning for computer vision: A brief review. *Computational intelligence and neuroscience*, 2018.
- 705 Wang, M., Yan, B., & Ngan, K. N. (2013). An efficient framework for image/video inpainting. *Signal Processing: Image Communication*, 28, 753–762.
- Wu, J., Lin, W., Shi, G., & Liu, A. (2013). Reduced-reference image quality assessment with visual information fidelity. *IEEE Transactions on Multimedia*,
710 15, 1700–1705.
- Xiang, S., Deng, H., Zhu, L., Wu, J., & Yu, L. (2019). Exemplar-based depth inpainting with arbitrary-shape patches and cross-modal matching. *Signal Processing: Image Communication*, 71, 56–65.
- Xie, P., Bilenko, M., Finley, T., Gilad-Bachrach, R., Lauter, K., & Naehrig, M.
715 (2014). Crypto-nets: Neural networks over encrypted data. *arXiv preprint arXiv:1412.6181*, .
- Xing, K., Hu, C., Yu, J., Cheng, X., & Zhang, F. (2017). Mutual privacy preserving k -means clustering in social participatory sensing. *IEEE Transactions on Industrial Informatics*, 13, 2066–2076.

- 720 Yan, W. Q., & Kankanhalli, M. S. (2015). Face search in encrypted domain.
In *Pacific-rim Symposium on Image and Video Technology* (pp. 775–790).
Springer. doi:10.1007/978-3-319-29451-3_61.
- Yan, X., Lu, Y., Liu, L., & Wang, S. (2018). Partial secret image sharing for
(k, n) threshold based on image inpainting. *Journal of Visual Communi-*
725 *cation and Image Representation*, 50, 135–144. doi:10.1016/j.jvcir.2017.
11.012.
- Yonetani, R., Naresh Boddeti, V., Kitani, K. M., & Sato, Y. (2017). Privacy-
preserving visual learning using doubly permuted homomorphic encryption.
In *International Conference on Computer Vision* (pp. 2040–2050).
- 730 Yu, J., Lin, Z., Yang, J., Shen, X., Lu, X., & Huang, T. S. (2018). Generative
image inpainting with contextual attention. In *IEEE Conference on Computer
Vision and Pattern Recognition* (pp. 5505–5514).