

Image Enhancement in Encrypted Domain over Cloud

ANKITA LATHEY, University of Winnipeg

and PRADEEP K ATREY, University of Winnipeg and State University of New York at Albany

Cloud-based multimedia systems are becoming increasingly common. These systems offer not only storage facility, but also high-end computing infrastructure which can be used to process data for various analysis tasks ranging from low-level data quality enhancement to high-level activity and behavior identification operations. However, cloud data centers, being third party servers, are often prone to information leakage, raising security and privacy concerns. In this paper, we present a Shamir's secret sharing based method to enhance the quality of encrypted image data over cloud. Using the proposed method we show that several image enhancement operations such as noise removal, anti-aliasing, edge and contrast enhancement, and dehazing can be performed in encrypted domain with near-zero loss in accuracy and minimal computation and data overhead. Moreover, the proposed method is proven to be information theoretically secure.

Categories and Subject Descriptors: K.6.5 [Security and Protection]

General Terms: Security

Additional Key Words and Phrases: Cloud Computing, Image Enhancement, Secret Sharing, Encrypted Domain Processing

1. INTRODUCTION

Cloud-based multimedia systems have seen a world-wide growth in recent years. These systems have two-fold benefits: 1) they store a huge amount of data (image/video) to be accessed, whenever required, and 2) they offer high-end computing infrastructure to process the data for various analysis tasks such as quality enhancement, object detection and tracking, and behavior analysis [Chu et al. 2013]. However, since cloud data centers (CDCs) are usually third party servers, these benefits come at the expense of security and privacy. To overcome the security and privacy issue, one can encrypt the data using traditional encryption methods such as Advanced Encryption Standard (AES) before sending it to CDCs. This solution works well for secured data storage over cloud, but it presents the challenge of processing the data in encrypted form.

The objective of this work is to investigate whether we can perform quality enhancement operations directly on the encrypted images over cloud. Consequently we found that some of the low-level processing tasks such as spatial filtering, anti-aliasing, unsharp masking, contrast enhancement and dehazing, which are generally used to improve the quality of the degraded images, can be performed in encrypted domain (ED) over cloud if Shamir's secret sharing (SSS) technique [Shamir 1979] is used as an encryption mechanism.

In the past, researchers have widely used the additive and multiplicative homomorphic properties of SSS to process encrypted images [Islam et al. 2009] for various analysis tasks. For instance, [SaghianNejadEsfahani and Sen-ching 2012] presented denoising of images using secret sharing

Majority of this work was undertaken at the University of Winnipeg and supported by the Natural Sciences and Engineering Research Council of Canada, Discovery Grant #408206.

Ankita Lathey's address: Department of Applied Computer Science, The University of Winnipeg, 515 Portage Avenue, Winnipeg, MB, R3B 2E9 Canada; email: lathey-a@webmail.uwinnipeg.ca; Pradeep K. Atrey's address: Department of Applied Computer Science, The University of Winnipeg, 515 Portage Avenue, Winnipeg, MB, R3B 2E9 Canada and Department of Computer Science, University at Albany - State University of New York, 1400 Washington Avenue, Albany, NY 12222 USA; email: p.atrey@uwinnipeg.ca and patrey@albany.edu

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.

© YYYY ACM 0000-0000/YYYY/01-ARTA \$15.00

DOI : <http://dx.doi.org/10.1145/0000000.0000000>

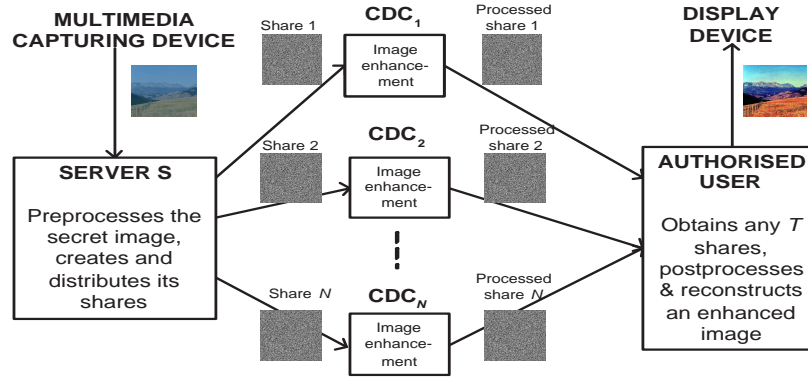


Fig. 1: An illustration of the working of the proposed method for image enhancement in ED over cloud

adapted for wavelet domain. [Upmanyu et al. 2009] proposed a secret sharing method for change detection in surveillance videos. However, in both works the proposals are only for carrying out integer addition and subtraction operations. Also, [Mohanty et al. 2012], [Mohanty et al. 2013] provided a method for preprocessing medical images such that real number analysis for addition/scalar multiplication (with terminating decimals only) is possible in ED. However, their method presents huge data expansion and the inability to perform division operations (particularly when the result of a division operation is non-terminating) in ED.

In this paper, we propose a novel and efficient method for performing arithmetic division operations for non-terminating quotients (involved in quality enhancement) over encrypted images¹. This allows an authorized user to reconstruct the improved quality images from CDCs. Our core idea is to use a (T, N) -SSS technique that divides the original (degraded) images (called ‘secret’) into N obfuscated images (called ‘shares’) (Fig. 1). The N shares are processed at N different CDCs for quality enhancement. In order to view the enhanced quality image, an authorized user first obtains the processed share images from any $(T \leq N)$ CDCs and then reconstructs the enhanced version of the original image. In our method, the user is not able to reconstruct the secret even if any $T - 1$ shares are available. As we intend to perform image enhancement tasks in ED over cloud, the real challenge lies in directly performing arithmetic operations (mainly division) with non-terminating decimal quotients involved in such tasks on the obfuscated share images at the CDCs. The proposed method addresses the above challenge and accomplishes the following goals:

- *Preservation of information theoretic security*: The advantage of using SSS over other methods is that it offers information theoretic security, which means that no matter how much computation power an adversary has, no information about the secret images can be obtained. Our goal is to adopt the SSS technique in a way that this property is preserved.
- *Minimal loss in accuracy*: Performing image enhancement operations in ED can result in some loss in accuracy compared to when these operations are undertaken in plaintext domain (PD). The goal of the proposed method is to minimize this loss. To this end, we propose four preprocessing schemes that provide zero or near-zero loss in accuracy.
- *Minimal overhead*: Secure processing of images comes at the expense of some computation as well as data overhead. The proposed method attempts to minimize both.

To the best of our knowledge, this is the first attempt to perform the quality enhancement operations directly in the spatial domain on the encrypted images over cloud. The proposed method is an improvement over existing methods [Mohanty et al. 2012], [Mohanty et al. 2013], [Upmanyu et al. 2009] for carrying out real number division operations (involving terminating decimals) in ED.

¹The earlier version of this work with preliminary results was published in [Lathey et al. 2013]

Table 1: Comparing the state-of-the-art methods for operations performed in ED with the proposed work

Works	Area(s) of Application	Type of multimedia worked upon	Add./ Sub.	Mult./ Div. (Integer & Real-Terminating)	Mult./ Div. (Real Non-Terminating)
[Islam et al. 2009]	Adding & Multiplying two encrypted images	Color/grayscale images	Yes	Integer	No
[Upmanyu et al. 2009]	Background subtraction	Surveillance videos/frames	Yes	No	No
[Hsu et al. 2009]	SIFT based feature extraction	Color/grayscale images	Yes	Integer	No
[Sadeghi et al. 2010]	Face recognition	Color/grayscale images	Yes	Integer	No
[Yogachandran et al. 2012]	Facial expression recognition	Color/grayscale images	Yes	Integer	No
[Mohanty et al. 2012], [Mohanty et al. 2013]	Rendering of medical images	3D medical images	Yes: Real Terminating	Yes: Real Terminating	No
[Chu et al. 2013]	Object Tracking	Video frames	Yes	Integer	No
PROPOSED WORK	Object Tracking	Color/grayscale images	YES	YES	YES

Workable applications of image quality enhancement using spatial filtering operations, namely low pass filtering (LPF), anti-aliasing filtering, unsharp masking/high boost filtering/edge and contrast enhancement along with dehazing, on digital images in ED over cloud are presented to demonstrate the utility of the proposed method. The techniques used for carrying out these image enhancement operations in ED are in compliance with the homomorphic properties of the chosen cryptosystem, SSS. Furthermore, a detailed Table is presented in the online appendix, comparing the possibility of performing the available state-of-the-art methods for various image enhancement operations taken into consideration.

The rest of this paper is organized as follows. In Section 2, we discuss the related works and what sets ours apart. Section 3 presents an overview of the proposed method. In Section 4 we describe the use of the proposed method with appropriate mathematical transformations for performing noise removal and anti-aliasing in ED. The application of the proposed method is extended in Section 5 to demonstrate the plausibility of performing unsharp masking for edge enhancement in ED along with histogram equalization as a postprocessing step for contrast enhancement and dehazing. Thorough security and performance analyses are also provided in Sections 4 and 5. Section 6 presents further remarks and Section 7 concludes our work.

2. RELATED WORK

Multimedia security has been extensively studied by researchers in the past two decades [Kankanhalli 2012]. In particular, the secret sharing technique has become very popular among researchers working in the area of secure domain multimedia processing. This technique was proposed by [Shamir 1979] and [Blakley 1979]. Many works thereafter emphasize the importance of the additive and multiplicative homomorphic properties of secret sharing for sharing and reconstructing secret images [Islam et al. 2009], [Chang et al. 2008]. There are very few works [Upmanyu et al. 2009], [Mohanty et al. 2012], [Mohanty et al. 2013] using SSS that involve direct processing of the encrypted secret data, along with the usual application of sharing and reconstructing the secret.

[Upmanyu et al. 2009] proposed a Chinese remainder theorem based secret sharing method for change detection in surveillance videos. Their system shattered each original video frame (secret) into multiple shares by using a shatter function, involving the scaling of each video frame's pixels by a factor and adding a random noise to the resultant pixels under the modulo prime domain. However, this work has two shortcomings. First, the proposal is made only for carrying out integer addition and subtraction operations. Second, the authors themselves admit that their system is inefficient in performing division operations, as it may lead to choosing a prime number in such a way that the size of the modulo domain is increased more than required. However, an alternative approach is proposed by using an additional computation server where the merge function is applied to respective residues obtained from other independent servers and the division/comparison is performed in

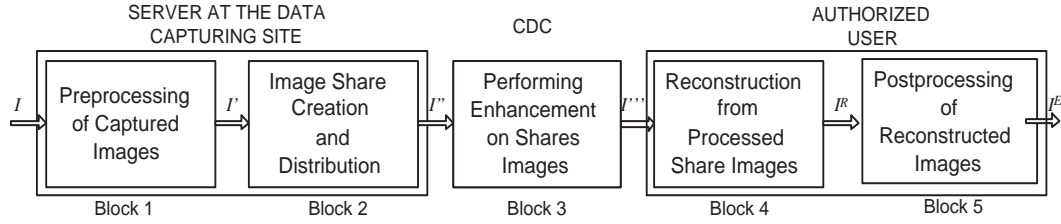


Fig. 2: Block-wise representation of the proposed method

the real domain. Hence, there is a suggested requirement to secure the intermediate information against attacks. Also, there is an additional communication overhead in sending the residues to the additional server and receiving the processed data back for this purpose.

The other works, [Mohanty et al. 2012], [Mohanty et al. 2013] attempted to provide a method for preprocessing the medical images in such a way that real number analysis for addition and scalar multiplication is possible in ED. One may argue that multiplication and division operations are inter-convertible, but [Mohanty et al. 2012], [Mohanty et al. 2013] involve multiplication with terminating decimals only.

In summary, the proposed method is different from [Upmanyu et al. 2009] and [Mohanty et al. 2012], [Mohanty et al. 2013] in preprocessing the original images in such a way that it is possible to perform division operations (irrespective of terminating/non-terminating decimals) on obfuscated share data and there is less or no overhead in transmitting the obfuscated share images to the CDCs, thus offering a more transmission-efficient solution. A detailed comparison of [Mohanty et al. 2012] with respect to the proposed work can be found in Sections 4.2 and 5.2. Note that as the work proposed by [Upmanyu et al. 2009] did not support the division operation, we have not compared our results with it. A brief comparison of the previous works presenting mathematical operations performed in ED can be seen in Table I.

3. AN OVERVIEW OF THE PROPOSED METHOD

A simple block-wise representation of our proposed method can be seen in Fig. 2. Block 1 applies less computationally expensive preprocessing operations on the original image (secret), I to produce a preprocessed image, I' . Block 2 creates share images of I' represented as I'' , which are completely arbitrary in nature and do not reveal any information. The share images are then sent to the CDCs, where they are processed for specific image enhancement operations in ED. After combining a threshold number of enhanced obfuscated share images from the CDCs, an authorized user is able to reconstruct an enhanced image, called I^R . Hence, the main feature lies in Block 1 where a suitable preprocessing function is applied to the image, so as to facilitate processing on obfuscated share image data at the CDCs in Block 3. This, in turn, produces the same results in ED as though image enhancement operations were performed on the original image data in PD. It is to be noted that another unit (assumed to be secure) can be added as Block 5, where some computationally less expensive postprocessing steps can be performed on the reconstructed image to obtain an image I^E , to display the enhanced image to the authorized user.

In the next two sections, we describe how the proposed method can be used to perform image quality enhancement operations in ED. The considered operations are: noise removal and anti-aliasing (in Section 4) and edge sharpening, contrast enhancement and dehazing (in Section 5).

4. NOISE REMOVAL AND ANTI-ALIASING USING HOMOMORPHIC LPF IN ED

Noise removal and anti-aliasing operations are performed by applying LPF on the images. The proposed method for performing LPF in ED consists of five major steps, which are described as follows:

Step 1 - Preprocessing the original images: Let a noisy digital image I , having g distinct pixel intensity (gray levels) values, comes to server S for secure distributed storage and retrieval. S pre-processes I (using either Scheme I or II as described in Section 4.1) to get I' . This is an essential step for making image data processing in the PD and ED compatible. Also, the preprocessing task depends on the type of operations to be performed on the share data.

Step 2 - Creating obfuscated images using SSS: Theoretically, (T, N) -SSS technique involves sharing a secret (an integer value) among a set of N participants in such a way that any $T \leq N$ participants can compute the secret, but a group of $T - 1$ participant(s) cannot do so [Shamir 1979]. The shares (or obfuscated images) are created using the following equation, which is evaluated under the modulo prime, p :

$$I''(x) = a_0 + \sum_{j=1}^{T-1} a_j x^j \mod p \quad (1)$$

where a_j coefficients are randomly chosen from \mathbb{Z}_p . The first coefficient a_0 is the secret that is divided into shares $(x, a(x))$ for different values of x (numerically described in Section 4.1).

In our method, the value of a_0 is the intensity value of the image (grayscale) pixels. In the case of the color images, to create the shares all the three color components, i.e. Red, Green and Blue, of each pixel can be combined as a secret (as ramp secret sharing in [Mohanty et al. 2012]), or can be taken as an independent secret channel (as in the proposed work). The number of obfuscated images that are created depends upon the number of participants, i.e. CDCs, where each obfuscated image is processed to carry out LPF.

Hence, Equation 1 is applied to the preprocessed image (I') of Step 1, in order to obtain the share image I'' . S provides the obfuscated images, I'' s, to the CDCs.

Step 3 - LPF on obfuscated images: Performing LPF in the spatial domain on an image I'' at any location (u, v) is the sum of $m \times n$ intensity values of the $m \times n$ neighborhood pixels centered around (u, v) divided by $m \times n$, and is represented as:

$$I'''(u, v) = \frac{1}{m \times n} \sum_{u=1, v=1}^{m, n} w(u, v) \times I''(u, v) \quad (2)$$

Hence, by replacing the value of each image pixel, $I''(u, v)$, with the average of the neighborhood intensity values defined by the filter mask, $w(u, v)$, a “smoothed” resultant image $I'''(u, v)$ with reduced transitions is obtained. Usually, the values of $w(u, v)$ are 1’s and 0’s. It could be a square (as used in our case) or a cross shape, with a well-defined center point. Also, the result of processing an image using Equation 2 is a real number in PD. However, the preprocessing in Step 1 makes the result of Equation 2 an integer value, which is needed to further facilitate LPF in ED.

Step 4 - Obtaining the enhanced LPF image: In order to obtain the enhanced images, an authorized user accesses the T number of I''' images from any T number of CDCs and uses the Lagrange Interpolation formula to reconstruct the image I^R .

Step 5 - Postprocessing the enhanced images: To obtain an error-free LPF secret image, there is a requirement to divide the reconstructed pixel values by a factor of $m \times n$, if the preprocessing is done using Scheme I (detailed in Section 4.1).

4.1. Implementation Challenges and Proposed Homomorphic Transformations: Noise Removal and Anti-aliasing in ED

The cryptosystem defined by SSS is considered to have additive and multiplicative homomorphic properties in the modular domain [Benaloh 1987]. However, LPF on image pixels requires performing an averaging/division operation on them (as per Equation 2). As division involves processing real number values, it may result in terminating or non-terminating decimal quotients. Hence, when the image shares are created using SSS and are processed directly for averaging operations in ED,

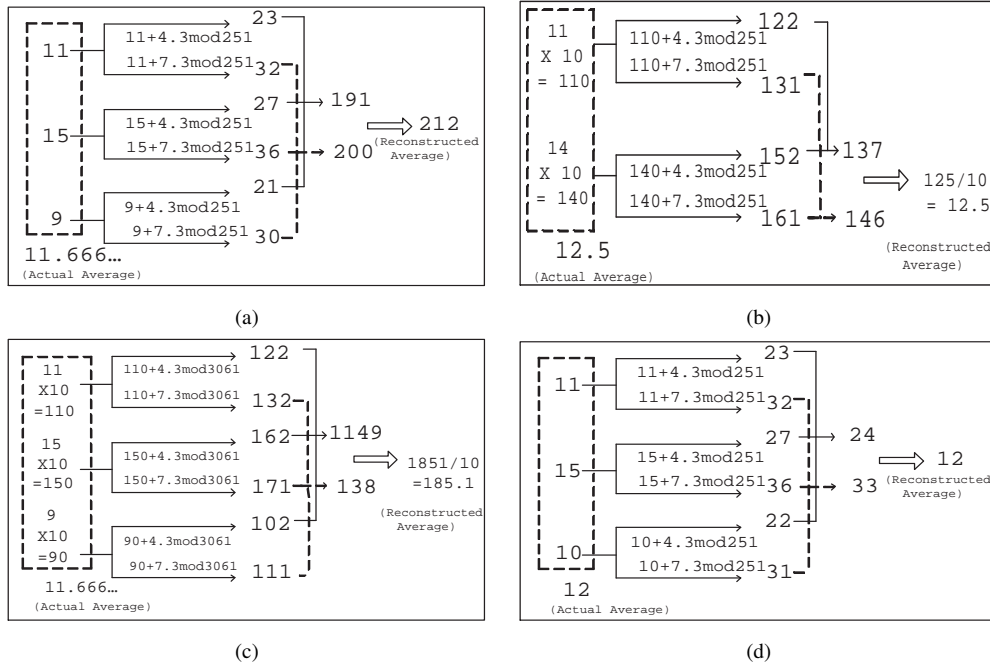


Fig. 3: Proposed homomorphic transformations:(a) Failed reconstruction for averaging of three numbers resulting in a non-terminating averaged value, (b) Successful reconstruction for averaging of three numbers resulting in a terminating decimal up to 1 decimal digit, (c) Unsuccessful reconstruction for averaging of three numbers resulting in a non-terminating decimal sequence, (d) Successful reconstruction for averaging of three numbers (completely divisible) in the modulo domain

reconstructing the exact averaged secret values as though the image pixels had been averaged in PD becomes inevitable. To demonstrate this let us look at Fig.3 (a).

Here, image pixels (secrets) are $\{11, 15, 9\}$. According to Equation 1, let a_0 be the secret, a_1 be 3, and the share numbers, i.e. x , be 4 and 7. All operations are performed under the modulo prime, i.e. 251 [Chang et al. 2008]. Thus, the 4th and 7th share values of the corresponding secrets are: $\{23, 27, 21\}$ and $\{32, 36, 30\}$, respectively.

The average is computed as: $\frac{11+15+9}{3} = 11.666..$ for the original image pixels (secrets), and $\frac{23+27+21}{3} \bmod 251 = 71 \times 3^{-1} \bmod 251 = 191$ and $\frac{32+36+30}{3} \bmod 251 = 98 \times 3^{-1} \bmod 251 = 200$ for the obfuscated image pixels (shares) under the modulo domain. Thus, reconstructing the averaged value using the Lagrange Interpolation formula, for $x = 4$ and $x = 7$ we get $[191 \times 7 \times 3^{-1} \bmod 251 + 200 \times 4 \times (-3)^{-1} \bmod 251] \bmod 251 = 212$. Clearly, the results of performing averaging in PD and ED are not equal.

One of the solutions for the real number analysis of addition and scalar multiplication in the modulo domain is provided in [Mohanty et al. 2012], where the author suggested that each pixel intensity value should be multiplied by a factor of 10^d , where d depends upon the precision of the desired decimal digits up to which we want to process the real numbers. The prime number should always be chosen as greater than $(255 + 51 \times 10^{1-d}) \times 10^d$. For example, in Fig.3 (b), the average (in PD) of image pixels (secrets) 11 and 14 is 12.5, i.e. a terminating sequence up to 1 decimal digit. So, to apply SSS, perform LPF and reconstruct the secret values, we need to preprocess the secrets by multiplying each of them by 10^1 (i.e. $d = 1$). Alternatively, in Fig. 3 (c), where the actual average of 11, 15 and 9 is 11.666..., i.e. a non-terminating sequence; even if we multiply the secrets by 10^1 (as performed for a terminating sequence in Fig.3 (b)), we can not recover the actual averaged values up to 1 decimal digit upon reconstruction. Hence, when the similar concept of preprocessing

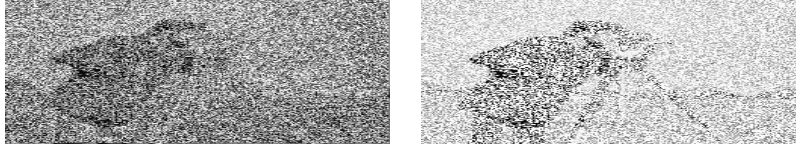


Fig. 4: Higher accuracy of reconstructed image with increased d in (a) $d = 1$, Prime used = 3061 & (b) $d = 2$, Prime used = 75611

as stated in [Mohanty et al. 2012] is applied for the division operation (involved in averaging), it can be verified that it works well for the terminating averaged quotients, while reconstructing the secret values for the non-terminating decimal quotients (where we cannot find the exact value of d) remains a challenge.

Furthermore, this can be visually examined by reconstructing (using [Mohanty et al. 2012]) the LPF image of *Cameraman* in Fig.4. Here, the greater the value of d , the higher the reconstructed secret values. But the non-terminating quotients are never reconstructed.

Also, [Mohanty et al. 2012] has a disadvantage as it leads to huge data expansion due to the preprocessing in the bit size of the share values, which can be a real trade-off for the transmission to the CDCs (explained in Section 4.2).

The proposed homomorphic transformations for digital images involve preprocessing the image data in such a way that averaging is performed on completely divisible values only, making the division operation homomorphic under the modulo domain. For instance, in Fig.3 (d), the sum of the original image pixels i.e. 11, 15 and 10 is 36, which is completely divisible by 3. Hence, if the original image pixels are as shown in Fig.3 (a) (averaged value is non-terminating), they can be preprocessed to make them equal to the ones shown in Fig.3 (d) (where the averaged value is an integer), thereby making the division operation produce the same results in both PD and ED.

The two schemes proposed for preprocessing the original noisy images, to perform LPF under ED are as follows:

Scheme I: Converting each pixel $I(u, v)$ to a multiple of $(m \times n)$ by,

$$I'(u, v) = I(u, v) \times (m \times n) \quad (3)$$

Scheme II: Changing each original intensity value to the nearest multiple of $(m \times n)$ by adding or subtracting a maximum of Δ values to or from its current value, where the range of Δ lies between 0 and $\lceil \frac{m \times n}{2} \rceil$ by,

$$I'(u, v) = I(u, v) \pm \Delta \quad (4)$$

4.2. Experimental Results and Analysis: Noise Removal and Anti-aliasing in ED

For experiments, the data capturing site (steps 1 and 2), CDCs (step 3) and the authorized user's site (steps 4 and 5) were simulated in a PC with the following configuration: Intel(R)core(TM) i5, 250 GHz, 64-bit processor with 6 GB RAM. MATLAB was used as an implementation tool. The detailed demos of the work can be found online at: <https://sites.google.com/site/ankitaresearchdemos/>. We discuss the results in the following two subsections.

4.2.1. Noise removal in ED. We present the experimental results of applying the proposed preprocessing schemes (Scheme I and Scheme II, as described in Section 4.1) for performing LPF over obfuscated images for noise removal using masks of different sizes. The dataset used for this experiment consisted of 118 grayscale images from a standard image dataset: *Database Release 2* [Sheikh et al. 2005], having different amounts of White Gaussian noise by varying standard deviation (σ) (provided explicitly in a file). The value of σ was chosen to be less than 1, as LPF does not produce considerable denoising effects for $\sigma \geq 1$.

LPF is performed on all 118 images using a mask of size 3×3 in both PD and ED. Hence, each pixel intensity value of the original noisy image (secret) is multiplied by 9 (as per Equation 3).

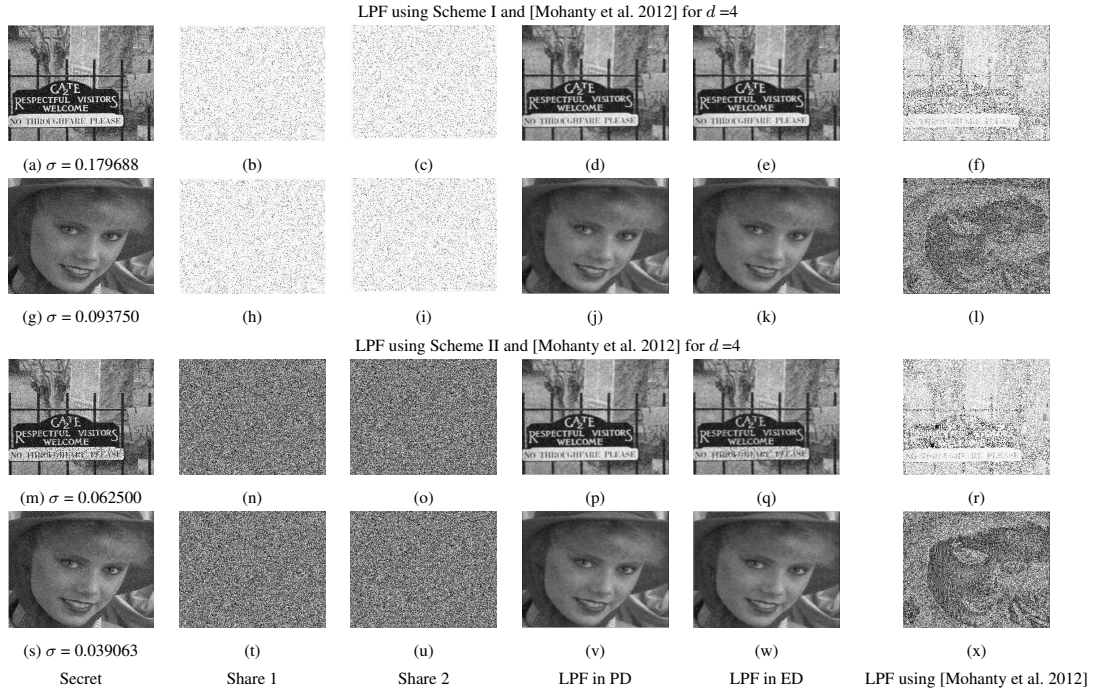


Fig. 5: Comparing LPF in ED

The first 2 rows in Fig.5 (a) and (g) show the original images (secrets). Fig.5 (d) and (j) represent the resultant images after performing LPF, on Fig.5 (a) and (g), respectively, in PD. Fig.5 (b)-(c) and (h)-(i) show the share images produced from Fig.5 (a) and (g), respectively. Remember that the intensity values of the share images are calculated using Equation 1. Fig.5 (e) and (k) represent the resultant images after performing LPF in ED on the corresponding share images of Fig.5 (a) and (g). Note that the visual effects of blurring and noise removal are exactly the same in Fig.5 (d)-(e) and (j)-(k).

Analogous to Scheme I, in Scheme II, LPF is performed on the same 118 images using a mask of size 3×3 in both PD and ED. Each pixel intensity value of the original noisy image (secret) is changed to its nearest multiple of 9 (as per Equation 4). Fig.5 (m) and (s) show the original images (secrets). Fig.5 (p) and (v) present the resultant images after performing LPF on Fig.5 (m) and (s), respectively, in PD. Fig.5 (n)-(o) and (t)-(u) show the share images produced from Fig.5 (m) and (s), respectively. Fig.5 (q) and (w) represent the resultant images after performing LPF on their corresponding share images. Note that the visual effects of blurring and noise removal are almost the same, as shown in Fig.5 (p)-(q) and (v)-(w).

The reconstructed images obtained using [Mohanty et al. 2012] with $d=4$ are shown in Fig.5 (f), (l), (r), and (x). It can be clearly seen that the proposed method presents better quality images compared to [Mohanty et al. 2012].

4.2.2. Anti-aliasing in ED. A brief introduction to the problem of aliasing or checkerboard effect in PD and how this can be realized in ED is shown in Fig. 6. It can be clearly seen that when we try to zoom-in to an image, its edges become jagged and it causes annoying artifacts called aliasing or checkerboard effect near the sharp transitions (mainly edges) present in the image.

One of the naive solutions to get rid of the checkerboard effect is to perform anti-aliasing filtering on the zoomed-in image. Anti-aliasing can be realised as LPF in the spatial domain. Hence, we present the experimental results when anti-aliasing is performed to remove the checkerboard effect



Fig. 6: Depicting the problem of aliasing or checkerboard effect in PD and comparing its removal using proposed Scheme I w.r.t. [Mohanty et al. 2013] in ED

from the obfuscated zoomed-in images (5 times), using a mask of size 3×3 (as bigger masks will incur more blurring). We tested our method with the following two standard datasets:

- In *License Plate Detection, Recognition and Automated Storage* [lic 2003], more than 400 images of license plates of different sizes are present. The images of the vehicles with a variety of license plates at different orientations have been collected.
- In *INRIA Person Dataset* [Dalal 2003], 300 images of people at various outdoor locations are present. Each one has a unique person or a group of people under different lighting/expressions/backgrounds.

The first 2 rows of Fig.7 show the results of applying Scheme I on one of the zoomed-in license plate and facial images, from the stated datasets. The images in column 2 (also the secret in our work) represent the results of zooming using the method of [Mohanty et al. 2013]. They clearly demonstrate the presence of checkerboard effect. One can easily identify that the results of applying Scheme I produce much better images in ED when compared to [Mohanty et al. 2013].

Furthermore, to compare the results of reconstructed anti-aliased zoomed-in images using Scheme I w.r.t. aliased zoomed-in images using [Mohanty et al. 2013], we conducted a user study where 30 enhanced images were randomly selected and the following 3 questions were asked to a group of 10 users. As a result of the study, the mean opinion score (MOS) of the group was calculated. MOS is the arithmetic mean of all the individual scores, and ranges from 0 (worst) to 5 (best). Fig. 8 (a) shows the results of the study. Here, Fig. 7 (f) and (l) are depicted by image no. 7 and 15.

- Q1: Has the checkerboard effect been removed using Scheme I w.r.t. [Mohanty et al. 2013]?

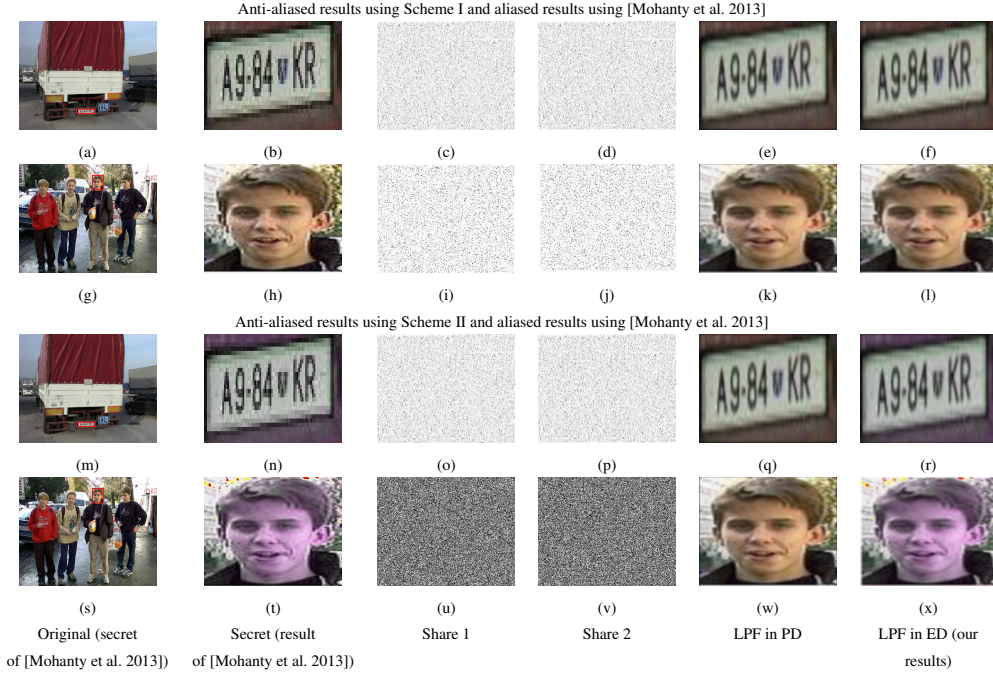


Fig. 7: Anti-aliasing in ED using Scheme I and Scheme II compared with [Mohanty et al. 2013]

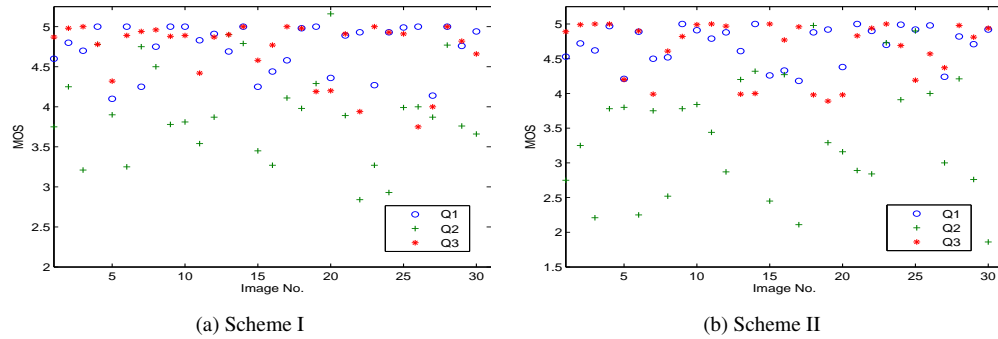


Fig. 8: A user study for comparing the anti-aliasing effects: Depicting MOS against 3 questions asked to a group of 10 users

- Q2: How would you rate the overall quality of the image obtained using Scheme I in ED?
- Q3: Is there a semantic similarity between the results using Scheme I w.r.t. PD?

It can be verified that most of the users found the results of Scheme I better than [Mohanty et al. 2013], particularly for checkerboard effect removal and semantic similarity. The MOS values for these 2 questions are in the range of [4-5]. The overall quality of the images fluctuates between MOS values of [2-5], because LPF has a blurring effect which at times produces results less appealing to the human eye.

Note that since we have multiplied the original image pixel by 9 and later scaled down the reconstructed LPF image pixels by dividing them by 9, there is no error introduced in this scheme.

The results of applying scheme II on the same zoomed-in license plate and facial images are shown in the last 2 rows of Fig.7. One can clearly identify that the results of Fig.7 (q) - (r) and Fig.7 (w) - (x) are also visibly comparable.

The differences between reconstructed images using Scheme I and Scheme II are due to some error introduced in performing LPF using Scheme II in ED due to the nearest multiple conversion according to the corresponding mask size(s), which is further detailed in Section 4.2.4.

To corroborate the similarity between anti-aliased images obtained using Scheme II and using Scheme I, we conducted another user study, where 30 images were randomly selected and compared for results produced using Scheme II w.r.t. Scheme I. The previously stated questions (Q1,Q2,Q3) were asked again to a group of 10 users and their MOS values are shown in Fig.8 (b). Here, Fig. 7 (o) and (t) are depicted by image no. 7 and 15. It can be verified that the MOS values of Q1 and Q3 are more inclined towards 5 and those of Q2 are in the range of [1.5 - 5]. This is because the nearest multiple conversion produces some color distortions, thereby decreasing the overall quality of the images for human perception.

4.2.3. Security analysis of the proposed method using Schemes I and II. The proposed method is based on SSS, which possesses information theoretic security. However, it is important to analyze whether the use of Scheme I and Scheme II makes any impact of the information theoretic security of the proposed method, which is what we do here.

Theorem 4.1 and Corollary 4.2 together prove that the proposed method using Scheme I represents an information theoretically secure cryptosystem as follows:

THEOREM 4.1. *If a secret image pixel a_0 , when shared using SSS, under \mathbb{Z}_p , is information theoretically secure, then another secret image pixel $a'_0 = a_0 \times \beta$ ($\beta \in \mathbb{I}$), when shared using SSS, under $\mathbb{Z}_{p'}$ (where p' is the first prime number greater than $p \times \beta$), is also information theoretically secure.*

PROOF.

For each of the original distinct gray level, g , (i.e. secret, a_0), under \mathbb{Z}_p of an image, (using Equation 1) there is an equal probability of it being any value between 0 and $(p - 1)$. This is given by:

$$Prob(a_0 = g)_{0 \leq g \leq p-1} = \frac{1}{p} \quad (5)$$

Similarly, for each of the distinct preprocessed gray levels, $g \times \beta$, (i.e. secret, a'_0), under $\mathbb{Z}_{p'}$ of the same image, it is equiprobable that they are of any value from the set $\{0, \beta, 2 \times \beta, 3 \times \beta, \dots, p' - 1\}$ of p number of values. This probability is given by:

$$Prob(a'_0 = g \times \beta)_{0 \leq (g \times \beta) \leq p'-1} = \frac{1}{p} \quad (6)$$

Note that in this case, a'_0 holds the values that are multiples of β . Even if an adversary divides all the values by β , the secret a'_0 can still be one of the p distinct values with equal probability ($1/p$). Since Equation 5 and Equation 6 yield the same probability value, the adversary does not get any information about the secret, and hence, it represents an information theoretically secure cryptosystem. \square

COROLLARY 4.2. *The proposed method using Scheme I represents an information theoretically secure system.*

PROOF. The proof lies along the same lines of Theorem 4.1 with $\beta = m \times n$. \square

Next, we analyze the security of Scheme II using Theorem 4.3 and Corollary 4.4.

THEOREM 4.3. *If a secret image pixel a_0 , when shared using SSS, under \mathbb{Z}_p , is information theoretically secure, then another secret image pixel $a'_0 = a_0 \pm \alpha$ ($\alpha \in \mathbb{I}$), when shared using SSS,*

Table II: Comparing data overhead (in terms of δ) required in transmitting a preprocessed image (using Scheme I) to CDCs

Mask sizes	3×3	5×5	9×9	10×10	16×16
δ_{Max}	12	13	14	15	16

under $\mathbb{Z}_{p''}$ (where p'' is the first prime number greater than $\lceil \frac{p}{\alpha} \rceil$), is also information theoretically secure.

PROOF. Similar to Theorem 4.1, for each of the original distinct preprocessed $g \pm \alpha$ gray levels (i.e. secret, a'_0) of an image, it is equally probable that they have any value between 0 and $(p'' - 1)$, and the probability is given by:

$$Prob(a'_0 = g \pm \lceil \alpha \rceil)_{0 \leq (g \pm \lceil \alpha \rceil) \leq p'' - 1} = \frac{1}{\lceil \frac{p}{\alpha} \rceil} \quad (7)$$

Since a'_0 holds the values that are multiples of α and its maximum value cannot be more than $p'' - 1$, there could only be $\lceil \frac{p}{\alpha} \rceil$ distinct values and a'_0 can hold these values with equal probability, therefore preserving the information theoretic security. Note that, although the number of distinct values reduces from p to p'' , this is due to the data loss, rather than any security loss. \square

COROLLARY 4.4. *The proposed method using Scheme II is an information theoretically secure system.*

PROOF. The proof lies along the same lines of Theorem 4.3 with $0 < \alpha < \frac{(m \times n)}{2}$. \square

4.2.4. Data overhead and error analysis of Scheme I and II. In the proposed method, Scheme I introduces no error, but it possesses some data overhead. On the other hand, Scheme II has no data overhead, but it introduces some error. Below, we first present the data overhead analysis of Scheme I, followed by the error analysis of Scheme II.

The efficiency of Scheme I can be expressed in terms of data bit overhead involved in the transmission of the share images to the CDCs as follows. According to Equation 3, the maximum pixel intensity value in the preprocessed image I' is $250 \times (m \times n)$. Let b be the number of bits used to represent this value. Then, the value of b is given as,

$$b = \lceil \log_2 250(m \times n) \rceil \quad (8)$$

Thus, the data overhead δ in transmitting I'' to the CDCs is bounded by $(0 \leq \delta \leq b)$ bits per pixel. Note that the p chosen must be greater than $250 \times (m \times n)$. Table II represents the maximum values of δ bits with increasing mask sizes.

Note that in general, a mask size of 16×16 is considered to be large enough for noise removal from images. Thus, for such a high mask value, δ is bounded by $0 \leq \delta \leq 16$ bits per pixel, which is more transmission efficient than [Mohanty et al. 2012],[Mohanty et al. 2013], where even for $d = 4$ (as mentioned in Section 4.1), δ is bounded by $(0 \leq \delta \leq 22)$ bits per pixel. Also, in [Mohanty et al. 2012],[Mohanty et al. 2013] there are some errors introduced for every color value of the pixel, which is contrary to our method, where the resultant LPF image is obtained without any errors by dividing the reconstructed averaged image pixels by $(m \times n)$, to get the same averaging results in PD and ED. The last column of Fig.5, shows the reconstructed secret images, preprocessed by multiplying each pixel intensity by 10^4 (for $d = 4$). Note that the secret images have different values of σ . It can be clearly seen that the higher the value of the noise (i.e. σ), the poorer the quality of the reconstructed images.

Furthermore, Table III compares the maximum values of bits δ_{max} with increasing values of d , required for higher precision of the reconstructed images using [Mohanty et al. 2012].

Table III: Comparing data overhead (with increasing d 's) required in transmitting a preprocessed image (using [Mohanty et al. 2012]) to CDCs

d	1	2	3	4	5	6	7
δ_{max}	12	15	18	22	25	28	32

Table IV: A comparison of the averaged image QMs for 118 LPF images using Scheme II for mask sizes: 3×3 , 5×5 & 7×7 w.r.t. [Mohanty et al. 2012] for $d = 4$ and mask size 3×3

QMs / Mask sizes	3×3	5×5	7×7	3×3 : [Mohanty et al. 2012] for $d=4$
NCC: The closer the value of NCC to 1, the lesser the difference between two images. This metric is used to quantify the closeness between the LPF images in PD and ED.	0.87	0.79	0.71	4.89
SC: The nearer the spread of SC to 1, the more the similarity in the structure of two signals. This metric is utilized to measure the quality of the LPF images in PD and ED.	1.33	1.46	1.54	6.04
LPSNR: The higher the value of PSNR for two images, the smaller the difference between them. This measure has been used to compare the loss in the PSNR values between the resultant LPF images in PD and ED.	2.40	2.72	3.19	10.73

In Scheme II, the error introduced by performing LPF on I' (obtained from Equation 3) for the mask size of $(m \times n)$ can be bounded as:

$$0 \leq \epsilon \leq \left\lceil \frac{m \times n}{2} \right\rceil \quad (9)$$

The error for the masks of sizes 3×3 , 5×5 and 7×7 is analyzed and compared for 118 images in Table IV. Three image quality metrics (QM) are used to further analyze the resultant images after performing LPF in PD and ED: Normalized Cross-Correlation (NCC), Structural Correlation/Content (SC) and Loss in Peak Signal-to-Noise-Ratio (LPSNR) [Lathey et al. 2013]. A pattern can be observed for these smaller masks, but the quality gets degraded with the larger mask sizes. The values are also compared for a mask size of 3×3 using [Mohanty et al. 2012] (for $d = 4$). Eventually, it corroborates the fact that the reconstructed LPF images using [Mohanty et al. 2012] have much more deviating averaged image QMs than the proposed scheme. Thus, Scheme II is more suitable for smaller masks. Since the range of the actual and preprocessed pixel intensity values is between $[0 - 250]$, this scheme gains full transmission efficiency in sending the same amount of data as the original image (i.e. 8 bits per pixel only), for the share images.

5. EDGE SHARPENING, CONTRAST ENHANCEMENT AND DEHAZING USING HOMOMORPHIC UNSHARP MASKING AND HISTOGRAM EQUALIZATION IN ED

The whole process of unsharp masking and histogram equalization can be realized with the following five major steps:

Step 1 - Preprocessing the original images: Add $k \times 255$ to each original pixel intensity value (to avoid the negative numbers problem in ED, stated in the following Step 3), followed by the similar preprocessing done in the proposed method for LPF, where S preprocesses I (by using Scheme III or IV as described in Section 5.1), to get I' .

Step 2 - Creating obfuscated images using SSS: The shares (or obfuscated images) are created using the same (T, N) - SSS scheme (Equation 1) for each of the R, G, B components of the image, which is evaluated in a finite field of a modulo prime number. Hence, similar to Step 2 in Section 4, share image I'' is created and S provides the obfuscated images, I'' s, to the CDCs.

Step 3 - Unsharp masking on obfuscated images over CDCs: Analogous to unsharp masking in PD, an edge enhanced image is obtained by using the following methodology in ED:

- (1) Perform smoothing or LPF on obfuscated (share) image, $I''(u, v)$, as per Equation 2. The result can be given as $I_{LPF}''(u, v)$.
- (2) Produce an edge image by subtracting $I_{LPF}''(u, v)$ from $I''(u, v)$ as:

$$I_{Edge}''(u, v) = I''(u, v) - I_{LPF}''(u, v) \quad (10)$$

This result of subtracting $I_{LPF}''(u, v)$ from $I''(u, v)$ is an image of higher value pixels in the areas of high contrast change (e.g. edges) and lower pixel values in the areas of uniformity. $I_{Edge}''(u, v)$ is an image with higher values (differences) in the areas affected significantly (by the smoothing) and low values in the areas where little change occurred. Thus, corresponds to a smoothed edge map of $I''(u, v)$. The pixel values of $I_{Edge}''(u, v)$ can be negative, which is dealt by adding $k \times 255$ as an extra preprocessing step (detailed in Section 5.1), so as to get similar effects in ED and PD.

- (3) The resulting difference image, $I_{Edge}''(u, v)$ is then added onto $I''(u, v)$ to effect some degree of sharpening, using a given constant scaling factor k that ensures the resulting image is within the proper range and the edges are not 'oversharp' in the resulting image. The ideal range for k is between $[0.5 - 1]$. The resulting obfuscated unsharp image is represented as:

$$I'''(u, v) = I''(u, v) + k \times I_{Edge}''(u, v) \quad (11)$$

This step enhances areas of rapid intensity change within the image whilst leaving areas of uniformity unchanged.

Step 4 - Obtaining the enhanced unsharp image: The enhanced images, I^R are obtained by the authorized personnel, using the Lagrange Interpolation formula, similar to the manner of Step 4 in Section 4.

Step 5 - Postprocessing of the reconstructed enhanced unsharp image: In order to obtain an error-free LPF secret image, there is a requirement to divide the reconstructed pixel values by a factor of $m \times n$ and subtract $k \times 255$, as per the preprocessing steps performed in Step 1 above. Then, by applying the automatic histogram equalization over the reconstructed image, as another postprocessing measure, an edge enhanced, better contrast image can be easily obtained.

5.1. Implementation Challenges and Proposed Homomorphic Transformations: Edge Sharpening and Contrast Enhancement/Dehazing in ED

To demonstrate the processes involved in performing unsharp masking in ED we use a block-wise depiction of the related steps in Fig.9. Here, each of the steps for getting the values of unsharp masking is performed under the modulo prime (chosen as 907) domain. The preprocessing is same as in Scheme I of Section 4.1. It can be clearly seen that the initially multiplied factor of the mask size i.e. $m \times n$ for LPF (i.e. 9 in this case), has to divide each of the reconstructed pixels in the final step so as to obtain the same result for the center pixel as 88 in performing the unsharp masking under ED.

The main challenge of implementing unsharp masking under the modulo domain lies in dealing with negative numbers resulting from Equation 10 in PD. It is rare to get a resultant negative number under the modulo domain. If a value of -2 is obtained as a final result by performing Equation 10 in PD, it will give $-2 \bmod 251$, i.e. 249 in ED. Hence, we suggest the preprocessing step, to add a value of $k \times 255$ to the original image pixels so as to bypass the effect of negative numbers under

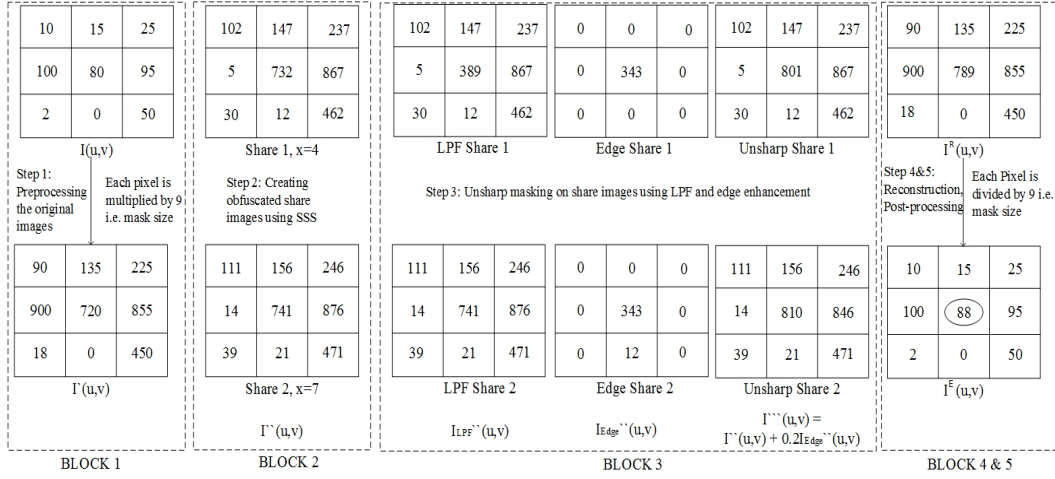


Fig. 9: A block-wise process of performing unsharp masking in ED over cloud

the modulo domain. In the process of reconstruction, subtracting by the same value i.e. $k \times 255$ leads to the retrieval of the original secret. Also, the prime chosen has to be greater than $(255 + (k \times 255)) \times m \times n$.

Similar to Section 4.1, there are two schemes for preprocessing the original images (secrets) in order to make unsharp masking in ED compatible with PD. They are given as:

Scheme III: Adding $k \times 255$ to each original intensity value and multiplying by the mask size, $(m \times n)$. In other words, add $k \times 255$ and then convert each pixel of $I(u, v)$ to a multiple of $(m \times n)$ by,

$$I'(u, v) = (I(u, v) + (k \times 255)) \times (m \times n) \quad (12)$$

Scheme IV: Adding $k \times 255$ to each original intensity value of $I(u, v)$ and converting it to the nearest multiple of $(m \times n)$ by adding or subtracting a maximum of Δ (same as defined in Section 4.1). In other words, increase the pixel value of $I(u, v)$ and round it to the nearest multiple of $(m \times n)$ as,

$$I'(u, v) = (I(u, v) + (k \times 255) \pm \Delta) \quad (13)$$

The difference in data overhead using Scheme II of Section 4.1, for LPF and Scheme IV of Section 5.1, for unsharp masking can be represented as,

$$\rho = (k \times 255), k \in [0.5, 1] \quad (14)$$

Here, Scheme III also leads to an error-free information theoretically secure solution with some data overhead. However, Scheme IV in this case represents an error bound information theoretically secure solution, with less data overhead compared to the corresponding Scheme III (as will be shown in Section 5.2.5).

5.2. Experimental Results and Analysis: Edge Sharpening, Contrast Enhancement and Dehazing in ED

5.2.1. Choosing the optimal mask size for unsharp masking. First, we try to find an optimal mask size for performing unsharp masking on 30 color images present in the dataset [Larson and Chandler 2010]. This helps in getting the minimal transmission overhead using Scheme III and reducing the error when using Scheme IV. The images have been computed for different amounts of ‘sharpness’ measured using average of gradients in X and Y directions. The three parameters chosen to measure the most suitable mask are averages (absolute values) of: percentage increase in

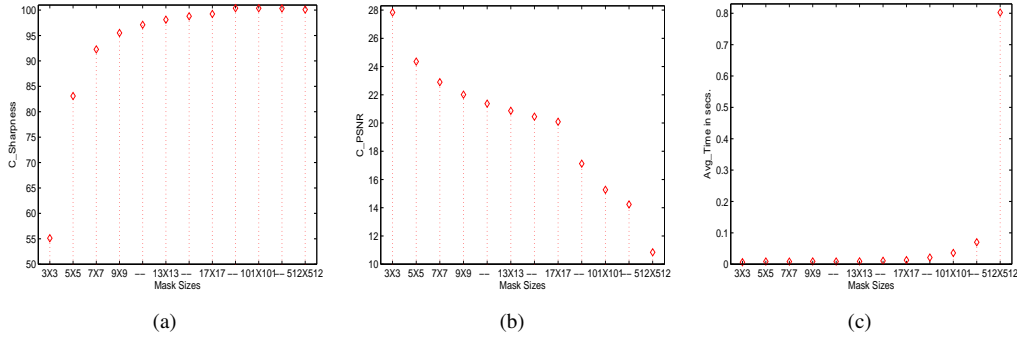


Fig. 10: Comparing (*C_Sharppness*)- left, (*Avg_PSNR*)- middle and (*Avg_Time*)- right, for optimal mask-size to perform unsharp masking.

the sharpness measure (*C_Sharppness*) with respect to the original images, average PSNR values (*Avg_PSNR*) of the resultant unsharp images with respect to the original images and average time taken (*Avg_Time*) to implement unsharp masking with increasing mask sizes, as shown in Fig. 10. Here, the values of the above stated parameters are depicted corresponding to 11 mask sizes: 3×3 , 5×5 , 7×7 , 9×9 , 11×11 , 13×13 , 15×15 , 17×17 , 51×51 , 101×101 , 512×512 . It can be clearly seen that the percentage increase (approx. 55.11%) in the sharpness value is very high after performing 3×3 unsharp masking, which gets further enhanced to approx. 83.08% and 92.26%, after performing 5×5 and 7×7 unsharp masking, respectively. Afterwards, there is a slight increase by 1% to 3% in the sharpness values. For changes in the average PSNR values with increasing mask sizes, it can be verified that there is a continuous decrease in the (*Avg_PSNR*) values with higher mask sizes. The nearer the value of PSNR to 30db, the better the quality of the enhanced image. Average changes in the time show an increasing trend with higher mask sizes. Hence, it can be concluded from Fig. 10 that for an image dataset [Larson and Chandler 2010], a mask of size 5×5 is best in terms of providing optimal results for the chosen parameters related to sharpness, time and most importantly, PSNR.

5.2.2. Edge and contrast enhancement in ED. We show the results of Schemes III and IV for computing the unsharp masking in ED and histogram equalization as a postprocessing step in order to obtain the resultant sharp-contrast enhanced image in ED. The experiments are performed on the database [Larson and Chandler 2010], where each of the original 30 images is present at 4 different levels of contrast distortion. The levels of distortion (1 to 4) are reported in the database as per 5000 subjective ratings from 35 different observers, in a separate file in the form of difference in mean opinion score (DMOS). DMOS is computed as the difference between the scores assigned to the original and distorted image.

Fig. 11 presents the results of Schemes III and IV. Fig. 11 (a) shows the original, distorted (low contrast) images (secrets) corresponding to distortion level 4 ($dmos = 0.371$), along with its corresponding R-plane histogram. Fig. 11 (b) represent the Share 1 image of the secret and the histogram distributions of its corresponding R-plane. For brevity, we have not shown Share 2 images which are very similar to Share 1 images. Fig. 11 (c)-(d) are the resultant images of performing edge and contrast enhancement in PD and ED (using Scheme III), respectively. It can be clearly verified that the histogram distribution of the resultant images in ED is the same as that of the resultant images in PD. Note that the visual effects of sharpening and contrast enhancement are also exactly the same in ED and PD. Also, the mask size chosen is the optimal one i.e. 5×5 , so we have multiplied each original image pixels by 25 and later scaled down the reconstructed unsharp image pixel by dividing them by 25. Hence, there is no error introduced in this scheme.

To measure the effect of the increase in the sharpness of images with different distortion levels, it can be seen in Fig.12 (a), that with increasing levels of distortion 1-4 there is a linear change

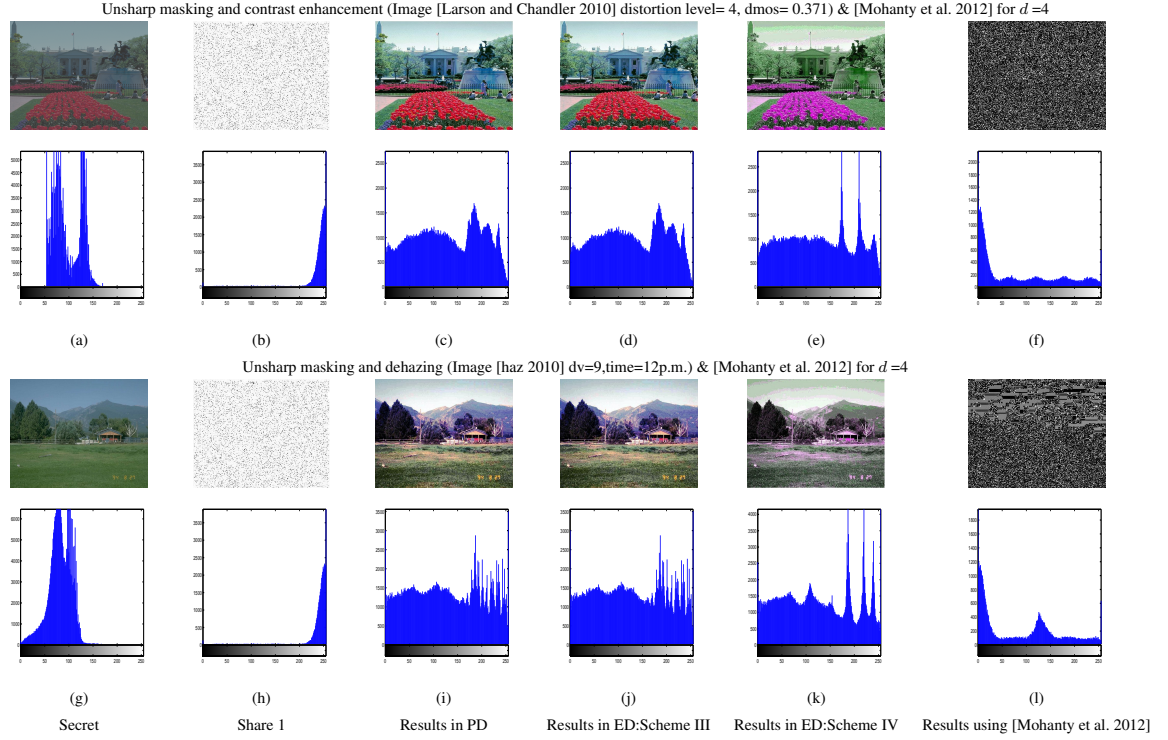


Fig. 11: Comparing results of unsharp masking, contrast enhancement and dehazing in ED

in the percentage of the average PSNRs of 30 enhanced images (reconstructed in ED). However, with the change in distortion levels 3-4 there is no percentage change in the average PSNR value of enhanced images. So, it can be concluded that distortion level 3 is the maximum distortion present in the database beyond which the average PSNR of the enhanced images cannot be improved. In other words, the effect of unsharp masking and contrast enhancement on average PSNRs beyond distortion level 3 will produce the same enhanced images, hence no change in the percentages.

Fig. 11 (e) represent the results of using Scheme IV for the same image along with the histogram distribution of its R-plane. Since the optimal mask size chosen is 5×5 , so we have converted each of the increased (by a factor of $k \times 255$, for $k = 1$) original image pixels to its nearest multiple of 25, there is some error introduced in this scheme. Note that the visual effects of sharpening and contrast enhancement are almost the same in PD and ED. Fig. 11 (g) show the resultant of the same enhancement operations on the image along with its histogram distribution of the R-plane using [Mohanty et al. 2012] for $d = 4$.

5.2.3. Dehazing in ED. We now show the results of applying unsharp masking in ED and histogram equalization (as a postprocessing step) for another image enhancement process, haze removal. A dataset of 100 images has been chosen from the “US Forest Service Air Quality Images” database [haz 2010], containing a spectrum series of regional haze visibility conditions observed at various sites for each monitored time of day. Each hazy image has a deciview (dv) number, representing the haziness index which is designed to be linear with respect to human perception of visibility. Higher dv values indicate more extinction and a corresponding decrease in visual range, indicating an increase in haziness.

Fig. 11 (g) shows a hazy image with dv=9 at 12 p.m., along with its processed images in PD and ED using Schemes III and IV in (i), (j), and (k), respectively. As stated, there is some error

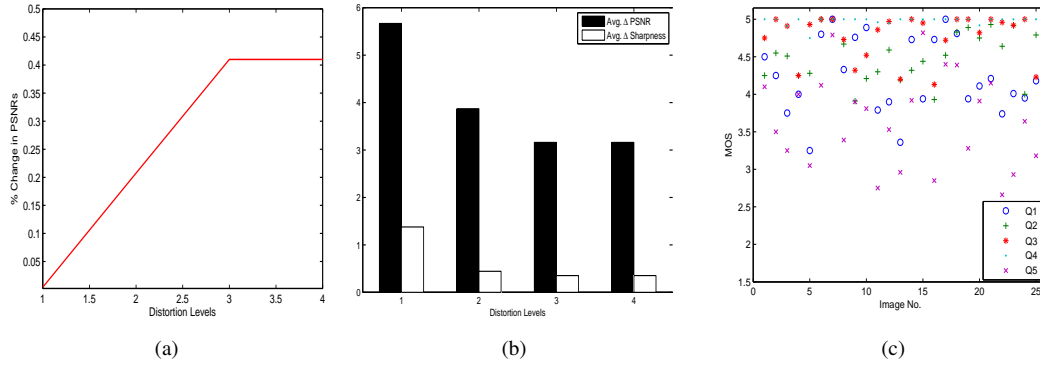


Fig. 12: (a) A comparison of percentage (%) change in the average PSNR values (after performing unsharp masking and contrast enhancement) for 30 images w.r.t. increase in distortion levels(1-4). (b) A comparison of the differences (Δ) in the average PSNR and Sharpness values (after performing unsharp masking and contrast enhancement) using Scheme III & IV, for 30 images w.r.t. distortion levels(1-4). (c) A user study, showing MOS of 10 users to compare the sharpening & dehazing results using Scheme IV w.r.t. Scheme III in ED.

introduced in this scheme due to nearest multiple conversion. However, if we examine the corresponding R-plane histogram distributions of the resultant images, it can be verified that the effects are comparable in PD and ED. Also, (l) shows the resultant of the corresponding image enhancement operations along with its histogram distribution of the R-plane using [Mohanty et al. 2012] for $d = 4$.

In order to analyze the difference in performance of Schemes III and IV, for performing edge and contrast enhancement in ED, the differences (Δ) in average PSNR and sharpness values of the resultant images can be seen in Fig. 12 (b).

Also, to compare the differences in performance of Schemes III and IV for sharpening and dehazing, we performed a subjective analysis of the resultant images obtained using both the Schemes in ED, by conducting a user study for the subjective analysis of the quality enhancement. 30 haze removed images were randomly selected and 5 questions were asked in a questionnaire. The questions were as follows:

- Q1:Has the haze been removed in ED w.r.t. PD?
- Q2:Has the contrast been enhanced in ED w.r.t. PD?
- Q3:Has the sharpness been increased in ED w.r.t. PD?
- Q4:Is there a semantic similarity between the results in ED w.r.t. PD?
- Q5:How would you rate the overall quality of the image obtained in ED?

Ten users provided their score on a scale of [0-5], where 0 represents no improvement/similarity and 5 represents full improvement/similarity, between the images in PD and ED. An average of the responses i.e. MOS is determined and can be seen in Fig. 12 (c). It can be easily verified that most of the scores are concentrated near the values of [4-5]. Only the overall quality is rated near the values between [2-4]. Hence, one may conclude that although the application of Scheme IV provides almost the same subjective analytical results when compared to Scheme III for haze removal, semantic similarity, contrast and sharpness enhancement in ED, the overall quality of the image becomes less appealing to the human eye because of color changes due to nearest multiple conversion.

5.2.4. Security analysis of the proposed method using Scheme III and IV. The following corollary proves the information theoretic security property of the proposed method using Scheme III:

COROLLARY 5.1. *Analogous to Theorem 4.1, if a secret image pixel a_0 , when shared using SSS, under \mathbb{Z}_p , is information theoretically secure, then another secret image pixel $a'_0 = ((a_0 + \gamma) \times \beta)$,*

($\gamma \in \mathbb{R}$) when shared using SSS, under $\mathbb{Z}_{p''''}$ (where p'''' is the first prime number greater than $(p + \gamma) \times \beta$), is also information theoretically secure.

PROOF. From Equation 5, it can be seen that the probability of guessing a secret by an adversary for each of the original distinct gray levels, g , (i.e. secret, a_0), under \mathbb{Z}_p , of an image is given by $\frac{1}{p}$.

Similarly, for each of the preprocessed gray levels, $((g + \gamma) \times \beta)$, (i.e. secret, a'_0), under $\mathbb{Z}_{p''''}$ of the same image, it is equiprobable that they are of any value from the set $\{(0 + \gamma \times \beta), (1 + \gamma \times \beta), (2 + \gamma \times \beta), \dots, p'''' - 1\}$ of p number of values. This probability is given by:

$$\text{Prob}(a'_0 = ((g + \gamma) \times \beta)_{0 \leq ((g + \gamma) \times \beta) \leq p'''' - 1}) = \frac{1}{p} \quad (15)$$

Here, since the probability values obtained using Equation 5 and Equation 15 are same, we conclude that it represents an information theoretically secure cryptosystem. \square

Note that, for the proposed method using Scheme III (unsharp masking in ED), the values of γ and β can be realized as: $\gamma = (k \times 255)$ and $\beta = (m \times n)$.

Now we consider the following corollary for security analysis of Scheme IV:

COROLLARY 5.2. *Following the Theorem 4.3, if a secret image pixel a_0 , when shared using SSS, under \mathbb{Z}_p , is information theoretically secure, then another secret image pixel $a'_0 = [a_0 + \gamma \pm \lceil \alpha \rceil]$, when shared using SSS, under $\mathbb{Z}_{p''''}$ (where p'''' is the first prime number greater than $(p + \gamma \pm \lceil \alpha \rceil)$), also possesses information theoretic security.*

PROOF. The proof is exactly same as Theorem 4.3.

Note that, for the proposed method using Scheme IV, the value of the prime chosen, p'''' has to be greater than $(250 + \gamma)$. Also the values of γ and α can be given as: $\gamma = k \times 255$ and $0 < \alpha < \frac{(m \times n)}{2}$. \square

5.2.5. Data overhead and error analysis of Schemes III and IV. In order to know the data bit overhead involved in the transmission of the share images to CDCs, consider Equation 12, where the maximum pixel intensity value in the preprocessed image I' is $(250 + (k \times 255)) \times (m \times n)$. Then, the value of b (the same as in Section 4.2) is given as,

$$b = \lceil \log_2[(250 + (k \times 255)) \times (m \times n)] \rceil \quad (16)$$

Also, the value of the data overhead δ (the same as in Section 4.2) is bounded by $(0 \leq \delta \leq b)$ bits per pixel. Note that the p chosen must be greater than $(250 + (k \times 255)) \times (m \times n)$. Also, for the chosen optimal mask size of 5×5 , the value of δ is bounded by: $(0 \leq \delta \leq 14)$, for $k = [0.5, 1]$.

The range of the preprocessed pixel intensity values, for a maximum value of k i.e. 1, is between $[0 - 500]$. Thus, the scheme gains almost full transmission efficiency in sending the share image data to the CDCs, i.e. only 9 bits per pixel. In other words, there is a constant data overhead of 1 extra bit when compared to Scheme II of Section 4.1. Also, the error is bounded by the same amount, ϵ as defined by Equation 9.

6. FURTHER REMARKS

6.1. Computational Efficiency: Delegation of Image Enhancement Operations to CDCs

The utility of the proposed method for delegating high end computing task to CDCs can be appreciated more if the major operations involved in an image enhancement process are performed over CDCs. There should be a minimal amount of pre/postprocessing operations at the server/client side. Hence, keeping such benefits in mind, we present in Table V a comparison of the number of operations required to be performed during the preprocessing step, at CDC, and after reconstruction as the postprocessing step for noise removal, edge sharpening, contrast enhancement and dehazing in ED.

Table V: A comparison of the number of operations performed in each block of the proposed method for LPF and unsharp masking in ED. Assuming $M' \times N'$ be the size of the original image.

Preprocessing	CDCs		Postprocessing
Noise removal and anti-aliasing- LPF: Scheme I			
$M' \times N'$ Multiplications	$\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$	no. of image blocks, with each block having $(m \times n)$ Additions + 1 division	$\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$ Divisions
Noise removal and anti-aliasing- LPF: Scheme II			
$M' \times N'$ Additions/Subtractions	$\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$	no. of image blocks, with each block having $(m \times n)$ Additions + 1 division	-
Edge sharpening, contrast enhancement and dehazing: Unsharp Masking and histogram equalization: Scheme III			
$M' \times N'$ Additions and Multiplications	$\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$	no. of image blocks, with each block having $(m \times n)$ Additions + 1 division. Followed by $M' \times N'$ Subtractions, Multiplications and Additions	$\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$ Divisions. Followed by histogram equalization involving $\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$ Additions and Divisions.
Edge sharpening, contrast enhancement and dehazing: Unsharp Masking and histogram equalization: Scheme IV			
$M' \times N'$ Additions and Multiplications	$\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$	no. of image blocks, with each block having $(m \times n)$ Additions + 1 division. Followed by $M' \times N'$ Subtractions, Multiplications and Additions	Histogram equalization involving $\left\lceil \frac{M' \times N'}{m \times n} \right\rceil$ Additions and Divisions.

Here, considering an image of size $M' \times N'$ the process of performing LPF for noise removal and anti-aliasing using Scheme I will involve only multiplication and division by a constant factor, $m \times n$ (mask size) as preprocessing and postprocessing steps, respectively. Depending upon the mask size(s) the CDCs will keep dividing the image into blocks of size $m \times n$ and then processing each block will involve $m \times n$ additions and divisions (averaging) for LPF. Clearly, multiplication/division by a constant is much easier than performing block-wise additions and divisions. Scheme II for LPF incurs nearest multiple conversion (depending upon the mask size) of each original pixel, which can be optimized by using techniques such as binary search and is cost effective to implement at the server side. Similarly, Scheme III and IV have an extra pre/postprocessing step of addition and subtraction of a constant term i.e. 255 to/from each image pixel in order to make edge enhancement possible in ED. Further utilization of automatic histogram equalization for contrast enhancement and dehazing as a postprocessing step can also be achieved in a less expensive manner at the server side by counting and the even distribution of the reconstructed image gray levels. CDCs perform block-wise averaging followed by subsequent steps of subtractions, multiplications and additions. Therefore, it can be verified that most of the pre/postprocessing steps for image enhancement in ED using our proposed method are computationally less expensive as compared to the operations performed at CDCs.

6.2. Limitations

In order to realize the importance of our method there is a need to understand the concept of using smaller masks and bigger masks in spatial domain for different image processing tasks. Depending upon the size of the filter, spatial filtering has two major usages in improving the quality of the image. First, small filters (especially, 3×3 , 5×5 , 7×7) help in reducing noise, which typically has sharp intensity transitions. Second, large filters (e.g. 9×9 , 11×11 , 16×16) help in smoothing false contours, thus reducing the irrelevant detail in an image. Furthermore, they enhance an image to get a gross representation of the region of interest. They facilitate the smaller objects in blending with the background, and larger objects become blob-like and easy to detect/track.

The aim of the proposed work is mainly for noise removal, anti-aliasing, edge sharpening, contrast enhancement, and dehazing image enhancement operations. We have experimentally verified that for different datasets used, the stated operations can be efficiently performed by choosing an optimal mask size from one of the small filters (3×3 , 5×5 , 7×7). Hence, the application of mask(s) with slightly increasing size(s) does not provide any major changes in the enhancement results.

Further, in order to empower the CDCs to perform $N \times N$ filtering task taking an LCM of all the mask size(s) and using the preprocessing schemes, Scheme I and Scheme III would provide

the suitable results in ED. We certainly admit that there will be a transmission overhead which is available in the existing methods as well. But, the novelty will still remain in being able to perform division operations directly over image pixels in ED. Also, for real time functioning of the method one may assume that there would be a communication between the Server, S and CDCs to ask for the mask size(s) in order to process the image data for any mask size.

7. CONCLUSION

We have presented an improved, efficient and secure method (as compared to [Mohanty et al. 2012], [Mohanty et al. 2013], [Upmanyu et al. 2009]) for enhancing images in ED. We emphasized the feasibility of performing the division operation (including non-terminating decimal quotients) in ED. In Sections 4 and 5 we showed the application of our method for various image enhancement operations including noise removal, anti-aliasing, edge sharpening, contrast enhancement, and dehazing. The online demos of the work can also be viewed at [www.acs.uwinnipeg.ca/pkatrey/...](http://www.acs.uwinnipeg.ca/pkatrey/) Throughout our work, the challenge of making the division operation compatible in both the real and modulo domains is addressed by adapting preprocessing schemes suitable for the image data. Schemes I and III lead to an error-free information theoretically secure solution with some data overhead, whereas Schemes II and IV represent an error bound information theoretically secure solution, with no or constant data overhead. Future work would be to examine the suitability of the proposed method for other image enhancement operations as well as for other higher level applications in video enhancement.

REFERENCES

2003. License Plate Detection, Recognition and Automated Storage. (2003). <http://www.zemris.fer.hr/projects/LicensePlates/english/results.shtml>.
2010. US Forest Service Air Quality Images. (2010). <http://www.fsvisimages.com>.
- M. Aguilar, C. Xlim, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey. 2013. Recent Advances in Homomorphic Encryption: A Possible Future for Signal Processing in the Encrypted Domain. *IEEE Signal Processing Magazine* 30, 2 (2013).
- M. Basu. 2002. Gaussian-based edge-detection methods-a survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*. 32, 3 (2002), 252–260.
- J. Benaloh. 1987. Secret sharing homomorphisms: Keeping shares of a secret secret. In *Proc. of Advances in Cryptology, Lecture Notes in Computer Science*, Vol. 263. Springer, 251–260.
- G. R. Blakley. 1979. Safeguarding cryptographic keys. In *Proc. of the IEEE National Computer Conference*. New York, USA, 313.
- A. Buades. 2006. *Image and film denoising by non-local means*. Ph.D. Dissertation. Universitat de les Illes Balears, Palma, Spain.
- A. Buades, B. Coll, and J-M. Morel. 2005. A review of image denoising algorithms, with a new one. *SIAM Multiscale Modeling & Simulation* 4, 2 (2005), 490–530.
- Y. Cai, K. Huang, T. Tan, and Y. Wang. 2006. Context enhancement of nighttime surveillance by image fusion. In *Proc. of 18th IEEE International Conference on Pattern Recognition*, Vol. 1. Hong Kong, 980–983.
- Y. Cha and S. Kim. 2006. Edge-forming methods for color image zooming. *IEEE Transactions on Image Processing* 15, 8 (2006), 2315–2323.
- C. C. Chang, C. C. Lin, C. H. Lin, and Y.H. Chen. 2008. A novel secret image sharing scheme in color images using small shadow images. *Elsevier Information sciences* 178, 11 (2008), 2433–2447.
- K.-Y. Chu, Y.-H. Kuo, and W.H. Hsu. 2013. Real-time Privacy-preserving Moving Object Detection in the Cloud. In *Proc. of the 21st ACM International Conference on Multimedia*. Barcelona, Spain, 597–600.
- K. Dabov, A. Foi, V. Katkovnik, and K. Egiazarian. 2007. Image denoising by sparse 3 – D transform-domain collaborative filtering. *IEEE Transactions on Image Processing* 16, 8 (2007), 2080–2095.
- N. Dalal. 2003. INRIA Person Dataset. (2003). <http://pascal.inrialpes.fr/data/human>.
- L. S. Davis. 1975. A survey of edge detection techniques. *Elsevier Computer graphics and image processing* 4, 3 (1975), 248–270.
- R. Fattal. 2008. Single image dehazing. In *ACM Transactions on Graphics*, Vol. 27. 72.
- R. C. Gonzalez and R. E. Woods. 2002. Digital image processing. (2002).
- K. He, J. Sun, and X. Tang. 2011. Single image haze removal using dark channel prior. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 33, 12 (2011), 2341–2353.

- M. D. Heath, S. Sarkar, T. Sanocki, and K. W. Bowyer. 1997. A robust visual method for assessing the relative performance of edge-detection algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19, 12 (1997), 1338–1359.
- C. Y. Hsu, C. S. Lu, and S. C. Pei. 2009. Secure and robust SIFT. In *Proc. of the 17th ACM international conference on Multimedia*. Beijing, China, 637–640.
- N. Islam, W. Puech, and R. Brouzet. 2009. A Homomorphic Method for Sharing Secret Images. *Springer Digital Watermarking* (2009), 121–135.
- N. Joshi and M. F. Cohen. 2010. Seeing Mt. Rainier: Lucky imaging for multi-image denoising, sharpening, and haze removal. In *IEEE International Conference on Computational Photography*. Cambridge, USA, 1–8.
- M. S. Kankanhalli. 2012. Introduction to Special Issue on Multimedia Security. *ACM Transactions on Multimedia Computing Communications and Applications* 8, 2S, Article 31 (2012), 31:1–31:2 pages.
- Eric C. Larson and Damon M. Chandler. 2010. Most apparent distortion: full-reference image quality assessment and the role of strategy. *Journal of Electronic Imaging* 19, 1 (2010), 011006. DOI : <http://dx.doi.org/10.1117/1.3267105>
- A. Lathey, P. Atrey, and N. Joshi. 2013. Homomorphic Low Pass Filtering Over Cloud. In *7th IEEE International Conference on Semantic Computing*. Irvine, USA, 310–313.
- M. Mohanty, P. K. Atrey, and W.-T. Tsang. 2012. Secure medical data visualization over cloud. In *Proc. of ACM International Conference on Multimedia*. Nara, Japan, 1105–1108.
- M. Mohanty, W.-T. Tsang, and P. K. Atrey. 2013. Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing. In *IEEE International Conference on Multimedia and Expo*. San Jose, USA, 1–6.
- S. G. Narasimhan and S. K. Nayar. 2003. Interactive (de) weathering of an image using physical models. In *Proc. of IEEE Workshop on Color and Photometric Methods in Computer Vision*, Vol. 6. France, 1.
- Y. Rao, W. Lin, and L. Chen. 2010. Image-based fusion for video enhancement of night-time surveillance. *International Society for Optics and Photonics. Optical Engineering* 49, 12 (2010), 120501–120501.
- A. R. Sadeghi, T. Schneider, and I. Wehrenberg. 2010. Efficient privacy-preserving face recognition. *Springer Information, Security and Cryptology* (2010), 229–244.
- M. Sayed Y. Luo SaghalianNejadEsfahani and S. C. Sen-ching. 2012. Privacy protected image denoising with secret shares. In *Proc. of the 19th IEEE International Conference on Image Processing*. Lexington, KY, USA, 253–256.
- Y. Y. Schechner, S. G. Narasimhan, and S. K. Nayar. 2001. Instant dehazing of images using polarization. In *Proc. of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Vol. 1. I–325 – I–332.
- A. Shamir. 1979. How to share a secret. *Communications of ACM* 22, 11 (1979), 612–613.
- H. R. Sheikh, Z. Wang, L. Cormack, and A. C. Bovik. 2005. LIVE Image Quality Assessment Database Release 2. (2005). <http://live.ece.utexas.edu/research/quality>
- Stephen M Smith and J Michael Brady. 1997. SUSANA new approach to low level image processing. *Springer International journal of computer vision* 23, 1 (1997), 45–78.
- K. Tan and J. P. Oakley. 2000. Enhancement of color images in poor visibility conditions. In *Proc. of IEEE International Conference on Image Processing*, Vol. 2. Vancouver, BC, Canada, 788–791.
- R. T. Tan. 2008. Visibility in bad weather from a single image. In *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*. Anchorage, AK, 1–8.
- M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar. 2009. Efficient privacy preserving video surveillance. In *Proc. of the 12th IEEE International Conference on Computer Vision*. Kyoto, Japan, 1639–1646.
- R. Yogachandran, C.-W. P Raphael, A. C. Jonathon, and J. P. David. 2012. Facial Expression Recognition in the Encrypted Domain based on Local Fisher Discriminant Analysis. *IEEE Transactions on Affective Computing* 4 (2012), 83 – 92. Issue 1.
- L. Zhang and X. Wu. 2006. An edge-guided image interpolation algorithm via directional filtering and data fusion. *IEEE Transactions on Image Processing* 15, 8 (2006), 2226–2238.

Online Appendix to: Image Enhancement in Encrypted Domain over Cloud

ANKITA LATHEY, University of Winnipeg
and PRADEEP K ATREY, University of Winnipeg and State University of New York at Albany

A. APPENDIX

A.1. Image Enhancement Techniques and their plausibility in Encrypted Domain

The problem of image enhancement can be formulated as follows: given a low quality input image and a high quality output image for specific applications, how can we make image clearer for automatic algorithms (detection, recognition, tracking, segmentation etc.) or subjectively better for human perception?

As emphasized in Section 1, there are various applications where digital images are acquired, processed, analyzed and used, such as surveillance, general identity verification, traffic, parking, malls, hospitals, schools, offices, criminal justice systems, satellite imagery, and other civilian or military image processing tasks. Carrying out image enhancement in PD is a difficult task [Rao et al. 2010], [Cai et al. 2006] due to the presence of high noise, low contrast and unsharp edges, we can not easily segment foreground-background form the scenes. Also, the environmental information affects the way people perceive and understand what has happened. Hence, dealing with fog, haze, rain, and snow in images is a daunting task due to poor illumination conditions. There are two main methods to process an image as defined by the domain in which the image is processed, namely, the spatial domain and the frequency domain. In the spatial domain, direct manipulation of the pixels is done. The frequency domain modifies the spatial frequency spectrum of the image as obtained by transform. Several techniques based on a combination of the two are also available. However, it is quite interesting to note that the same enhancement technique can be implemented in both domains, yielding the same results.

It is established that spatial domain based techniques are conceptually easier to understand and have lower time complexity which favors real time implementations. Therefore, our proposed work benefits from the simplicity of these techniques. However, the task the performing a PD equivalent of the image enhancement operations in ED is more challenging due to the transformation of original pixels into completely random values after encryption. Hence, the unavailability of a fully homomorphic cryptosystem is a limitation [Aguilar et al. 2013]. Only those image processing operations which can be sub-divided into four basic arithmetic operations: addition, subtraction, multiplication, and division, can be applied utilizing the homomorphic properties in ED.

We now provide a comparison in Table VI of various classical and contemporary methods available for image enhancement - noise removal, checkerboard effect removal/ anti-aliasing, edge sharpening, contrast enhancement and dehazing, along with their feasibility in ED, based on mathematical operations involved in the respective methods.

Table VI: A comparison of the feasibility of various image enhancement methods in ED

Name of Technique	Main operations used	Feasibility
Noise removal methods		
Average or Low Pass filtering [Gonzalez and Woods 2002]	Addition, Division	Yes
Weighted Average filtering [Gonzalez and Woods 2002]	Addition, Division	Yes
Median filtering	Addition, Division, Sorting/Comparison	No
Discrete Wavelet Transform (DWT) [SaghaianNejadEsfahani and Sen-ching 2012]	Addition, Subtraction, Multiplication, Thresholding	Partially
Non-local (NL) means algorithm [Buades 2006], [Buades et al. 2005]	Addition, Subtraction, Multiplication, Division, Comparison, Partial differential equations, statistical correlation between pixels in vicinity	No
BM3D: 3D block matching (grayscale) [Dabov et al. 2007]	Addition, Subtraction, Multiplication, Division	Yes
CBM3D: 3D block matching (color) [Dabov et al. 2007]	Addition, Subtraction, Multiplication, Division: for individual luminance value	No
Anti-aliasing filtering or checkerboard removal methods		
Gaussian Low Pass filtering [Gonzalez and Woods 2002]	Addition, Division	Yes
Median Low Pass filtering [Gonzalez and Woods 2002]	Addition, Division, Sorting/Comparison	No
Alternating Direction Implicit method [Cha and Kim 2006]	Addition, Subtraction, Multiplication, Division, Comparison, Partial differential equations, Polynomial curve equations	No
A new interpolation method [Zhang and Wu 2006]	Addition, Subtraction, Multiplication, Division, Minima, Mean square error	No
Edge sharpening, contrast enhancement and dehazing methods		
Gaussian High Pass filtering [Gonzalez and Woods 2002]	Addition, Subtraction, Division	Yes
Unsharp Masking	Addition, Subtraction, Multiplication, Division	Yes
Some sequential methods [Davis 1975]	A priori knowledge and coherence is needed	No
SUSAN method [Smith and Brady 1997]	Addition, Subtraction, Division, Maxima/Minima based on near pixel comparison	No
Other GHPF e.g. Canny [Basu 2002], [Heath et al. 1997], [Gonzalez and Woods 2002]	Addition, Subtraction, Division: Identification of zero crossings replacing subtraction operation for first order derivative	Yes
General contrast stretching: linear mapping, histogram stretching and equalization, and gamma correction [Gonzalez and Woods 2002]	Addition, Counting, Division: works on direct pixel correlations	No
Polarization filtering [Schechner et al. 2001]	Addition, Subtraction, Multiplication, Division, Comparison for finding airlight and creating depth-map of images, Trigonometric and logarithmic functions	No
Physical Models [Narasimhan and Nayar 2003]	Addition, Subtraction, Multiplication, Division, Maxima/Minima, Exponential functions, Depth-map estimation, Interactive contrast enhancement	No
Maximizing contrasts: direct transmission [Tan and Oakley 2000], [Tan 2008]	Addition, Subtraction, Multiplication, Division, Maxima/Minima for contrast enhancement, Classification of each RGB pixel based on it's mapping in a cube	No
Single image dehazing [Fattal 2008]	Addition, Subtraction, Multiplication, Division, Maxima: airlight component, Classification: by relating nearby pixels	No
Computational photography [Joshi and Cohen 2010]	Addition, Subtraction, Multiplication, Division, Maxima/Minima, per-pixel selectively measure for local area selection, contrast enhancement by color remapping within certain range	Partially
Single image dehazing: dark channel prior [He et al. 2011]	Addition, Subtraction, Multiplication, Division, Maxima/Minima, Uses a Prior: haze-free images contain some pixels whose intensity is very low in at least one color channel, trigonometric and exponential functions	No