**Responses to the reviewers’ comments**

Dear Editor and Reviewers:

Thank you very much for your time in reviewing our manuscript "Image Enhancement in Encrypted Domain over Cloud (TOMCCAP-2014-0032)" and giving us the opportunity to revise the manuscript. We have now revised our manuscript in response to all the reviewers' comments. The revised manuscript along with a response document is resubmitted for your second review.

Please note that in this version of the paper we have used the newly introduced ACM TOMM template (which allows 22 pages).

Thanks and best regards,

Authors

**Reviewer #1:**

Comment 1: The problem the authors are trying to solve is timely and important for the research community. However, some deficiencies are in this paper.

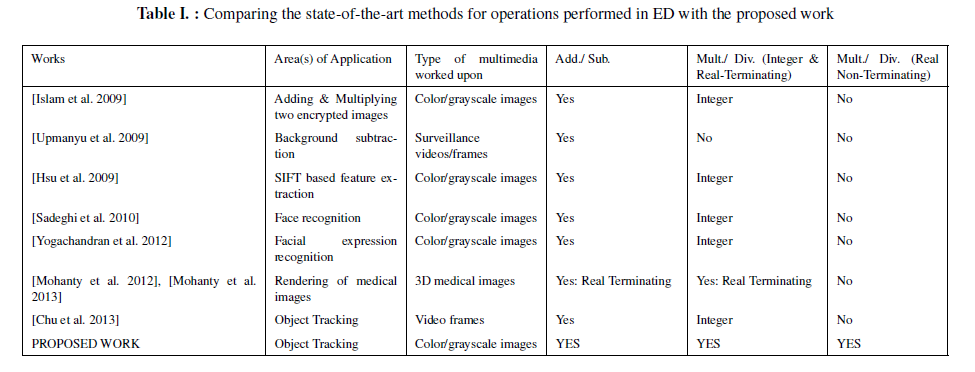
Response: Thank you very much for reviewing this manuscript and for providing constructive comments. Your comments and suggestions helped us to improve the quality of the paper.

Comment 2: Author mainly propose a slight modification to the Shamir's Secret Sharing (SSS) method. The novelty is low.

Response: We greatly appreciate the comment. However, we would like to mention that the main aim of the work is to utilize SSS by suitably adapting it for image data to enhance it directly in encrypted domain. Moreover, the novelty of our work lies in performing division operations (used in averaging for both real terminating and non-terminating decimal quotients).

Further, we have clearly mentioned the novelty of our work in the last paragraph of Page 2, as: “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.”

Also, we understand that in the previous version there might not be a clear mention of how our work is different in the area(s) of application w.r.t. the other works, so we have provided an updated table (Table I on page 3) in the revised version as:



Comment 3: Meanwhile, some potential weaknesses need to be addressed, for example:

a) the encryption client needs to know the operations performed in the cloud server in advance  and do the corresponding pre-processing, which might be not feasible in real case. For example, we want to do 3\*3 smoothing, then multiply 9 at the first step. However, how about if we want to change the algorithm in Cloud later? It seems we need to encrypt all the data with different pre-processing again.

b) How about if we want to apply both 3\*3 and 5\*5 filter in the cloud. One way to solve it is to encrypt same image with different pre-processing, but I think that is not efficient.  
    If you only want to encrypt the images once, you might need to multiply 9\*25 for pre-processing, which I think is also a very large overhead. And, scheme II seems doesn't work in this setting. It might cause large reconstruction errors.

Response: Thank you for the suggestion. In order to address this comment we have added a new Sub-Section, 6.2: Limitations under Section 6: FURTHER REMARKS, as under:

“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 × 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 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.”

Comment 4: What are the major contributions of the paper?

a) In this paper, the encryption methods that authors proposed mainly based on the Shamir's Secret Sharing (SSS) method. However, traditional SSS only works on positive integers (both inputs and calculated result need to be positive integers).

b) To solve the problem that division might cause non-integer (LPF), authors proposed two ways to solve it.  
For an integer going to be divided by N,  
  Scheme I: First multiply the integer by N  
  Scheme II: find the nearest number which can be well-divisible by adding or subtracting a value delta.  
  
c) To further solve the problem that the calculated value might be negative (Edge Sharpening, Contrast Enhancement), authors propose add k\*255 value and combined previous two schemes to form the Scheme III and IV.

Response: We appreciate the comments. And, thank you for your valuable time in having such an in depth mathematical understanding of our work, thus, providing a constructive feedback about major contribution(s).

**Reviewer #2:**

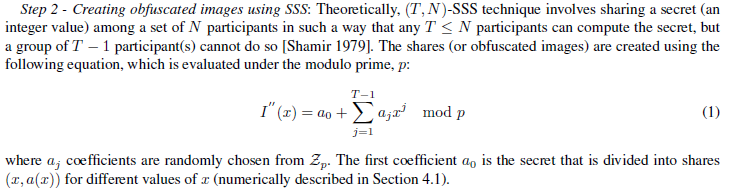
Comment 1: This paper proposed a novel an efficient framework for arithmetic division operations for non-terminating quotients. As far as I know, this paper is the first to perform image quality enhancement directly on spatial domain over cloud. That means the idea of this paper is novel.

Response: We thank the reviewer for reviewing the manuscript and providing the constructive comments. Your valuable comments and suggestions helped us to improve the quality of the paper by incorporating the suggested measures.

Comment 2: The weakness of this paper is that the theory of this paper is not strong. It seems the paper simply applies the cloud framework on certain types of image enhancement tasks.

a) I suggest the authors clearly illustrate the technique part in the revised version (use a new section).

Response: We appreciate the comment. We have made the changes to clearly state the theoretic application of SSS and it can be seen on Page 5, as under:



We would also like to clarify that we have provided the implementation details of the technique used in the form of separate sections i.e. Section 4.1 and Section 5.1. Further, Fig. 3 and Fig. 9 provide an insight about the working of the proposed method utilizing step wise solution using numeric examples.

b) Besides, please clearly claim the hardware that are used in cloud framework.

Response: Thank you for the comment. We would like of clarify that at the beginning of the Section 4.2, we have mentioned the details of the system configuration used as “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 an implementation tool.”

c) Finally, more experimental images should be presented in the revised version.

Response: We appreciate the comment and would like to mention that due to space constraints we could not provide more experimental images in the paper. However, in Section 4.2, we have provided a link for the available online demos of the proposed work as “The detailed demos of the work can be found online at: <https://sites.google.com/site/ankitaresearchdemos/>.”

Comment 3: This paper made three contributions in Encrypted image enhancement domain: 1) The advantage of using SSS over other methods is that it offers information theoretic security.  2)  Performing image enhancement operations in ED can result in some loss in accuracy compared to when these operations are undertaken in plaintext domain. 3)  Secure processing of images comes at the expense of some computation as well as data overhead  
Response: We appreciate the comments. And, thank you for your valuable time in having such an in depth mathematical understanding of our work, thus, providing a constructive feedback about major contribution(s).

**Reviewer #3:**

Comment 1: In this paper, a novel and efficient method for performing arithmetic division operations for non-terminating quotients over encrypted images. The proposed method is an improvement over existing methods for carrying out real number division operations in ED. And the techniques used for carrying out these image enhancement operations in ED are in compliance with the homomorphic perperties of  the chosen cryptosystem. Moreover, the proposed method is more generic-purpose than the state of the arts. The experimental results are convincing. And the overall writing is clear. Some polish are needed for figure 2 and 3 to make the chart looks more professional.  
Response: We thank the reviewer for reviewing the manuscript and providing the constructive comments. Your valuable comments and suggestions helped us to improve the quality of the paper by incorporating the suggested measures. We have enlarged the figures and tried our level best to make them look clearer.

We have used MS VISIO for creating high quality .eps figures to be embedded into LaTex files. Also, we would greatly appreciate if the reviewer may suggest any other tool to be used for creating high quality figures.

Comment 2: Image enhancement in encrypted domain is a new topic, especially in cloud computing area. This paper presents an approach to preserve the information theoretic security while minimizing the loss in accuracy and overhead during image enhancement in encrypted domain.  
Response: We thank the reviewer in recognizing the importance of the topic and realizing our research as an important contribution to the secure multimedia - cloud computing domain.

Comment 3: The first attempt to perform the quality enhancement operations directly in the spatial domain on the encrypted images over cloud.  
Response: We appreciate the comments. And, thank you for your valuable time in having such an in depth mathematical understanding of our work, thus, providing a constructive feedback about major contribution(s).