I. INTRODUCTION

Social Networks (SNs) such as Facebook, Twitter or Instagram are only a few examples of the most used Internet applications all over the world. A recent study shows that Facebook has at least 1.71 billion active users per month. Moreover, according to that study, it is estimated that more than 300 million photos per day are being uploaded. Most SN users have the tendency to share photos. There are several works that are focused on the reason for sharing personal information such as photos on SNs from a sociological perspective. These studies found out that most users share photos on SNs to seek affection. Nevertheless, users are aware of the risks of their actions which might reveal personal aspects of their lives. Due to this, users usually weigh the risks of disclosing private information against benefits of not doing it. Both security and privacy issues have been pointed out in several papers as unsolved and challenging problems. Specifically, in the privacy domain, some authors have addressed photo sharing [1] as an open problem in SN. This problem arises when users take photos they have access to and increase the audience of the photo by re-sharing it. For instance, imagine that Alice shares a photo with her friends, and later, Bob—who is a friend with Alice—re-shares it with his own friends, thus increasing the audience to his own friends as well. Essentially, this circumstance is given because the privacy policies that Alice has previously defined are applied only to her public Domain and are not attached to the objects she shares out.

II. LITERATURE REVIEW

There are many techniques for securing images. In this paper, few of the prominent existing research work are reviewed to cover all the available image security techniques such as image transformation, image encryption, and image steganography.  
2.1 Image Transformation In image transformation, digital image is taken as an input and produces another image as its output to enhance the security level of an image. The first image encryption method we have discussed in the below table is block-based image transformation. It divides input image into blocks, which were rearranged into a transformed image using their respective transformation algorithm. Their results show’s that increasing the number of blocks by dividing image into smaller blocks results in a lower correlation.
and higher entropy. Another type of image transformation like Fractional Fourier Transformation (FRFT) and wavelet transform are also covered in the following table.

2.2 Image Encryption Image encryption is the process of converting an input image into another random image that is hard to understand. This can be done by using key or without key. There are numerous image encryption methods available to make transmission of images more secure. Different types of image encryption methods are discussed below.

2.3 Image Steganography- Steganography is a data hiding technique used to protect multimedia data. It hides information within other information to make it impossible for any unauthorized user to identify presence of any secret information. Steganography uses different types of carriers like text, digital image, or video, of which digital images are the most popular. Image steganography works slightly different from that of image cryptography. The cryptography keeps the contents of a message secret whereas the steganography keeps the existence of a message secret. We have analyzed and tabulated various image steganography approaches used for securing images.

2.4 Other Techniques for Image Security Nowadays, many new methods for improving the security level of images have been proposed and every day new image security technique is evolving.

2.5 Image encryption using compression and encryption: There are mainly three ways of achieving image security using this approach, the first way is compression followed by encryption, second way is encryption followed by compression and last is joint compression and encryption.

III. IMPLEMENTATION

Existing process
In online social network (OSN) user’s resource may contain the privacy of other resources. Most of the social networking sites provide features that allows user to easily upload and post photos on social network. Many privacy violations occur in current online social network which becomes a serious problem. Unfortunately photos that a user is tagged in, have very few privacy control. A nowadays researcher focuses on how to integrate into co-worker’s willingness of privacy when setting access rule for resource.

Proposed methodology
In this paper, we study the situation when a client shares a photograph containing people other than himself/herself. We proposed a system where photo can be shared in a secure way. Proposed framework can help clients to effortlessly and appropriately design security settings. The existing system has the individual face recognition system installed with each user, which is very time-consuming. Proposed system has a centralized FR engine in charge of recognizing all users over a large OSN. Effectiveness and Flexibility is good of Proposed Solution.

I) Client End
Front Page – Using web application for the user to interact, download, and upload images. Module to split the two images into 4 equal parts respectively. Function to apply hashing technique to enhance the security. Module to overlap the two split images into a single image. Module to encrypt the overlapped single image into a shared image. Apply RSA algorithm with a key

II) Server end
Module to provide interface for the user to enter a key to decrypt the shared image. Module to decrypt the shared image in order to obtain a single image which was overlapped. Function to split overlapped image as two separate split share of images. Function to compare the hash values which were generated during the encryption process
Function to obtain back the original confidential images which were initially uploaded from the client end.

III) Functionalities
Upload image – This function deals with the end user, who has to load the images which are to be transmitted securely. This just loads the image to the interface provided. Send image – This includes the function which actually performs all the computation that are required to encrypt the image and transmit the image from one end to the other end. Download image – The options or the interface is provided to download the transmitted images that are been sent from the other end. The shared image is downloaded. Meanwhile, the download function also provides the interface or the input method in order to enter the secret key which is been sent from the sender site. After entering the password or key the processing of decryption takes place internally and final original image will be received at the receiver end.

IV. CONCLUSIONS
How the images are being transmitted from one end to other securely, providing different security methods at different stages are being presented and discussed in this paper. However there are stages differentiated at both client end and the server end with appropriate modules. Based on these things we would recommend that this project would work successfully and efficiently.

Future enhancement
In this paper we study the situation when a client shares a photograph containing people other than himself/herself. We proposed a system where photo can be shared in a secure way. Proposed framework can help clients to effortlessly and appropriately design security settings. The existing system has the individual face recognition system installed with each user, which is very time-consuming. Proposed system has a centralized FR engine in charge of recognizing all users over a large OSN. Effectiveness and Flexibility is good of Proposed Solution.

REFERENCES