Digital image information encryption based on compressive sensing and double random-phase encoding technique

Etienne Cuche, Frederic Bevilacqua, and Christian Depeursinge
Institute of Applied Optics, Swiss Federal Institute of Technology, CH-1015 Lausanne, Switzerland

Presenter: Nitin Rawat

Considering the threat of accessing and tempering data by an unauthorized person, a secure transmission of multimedia information like image data using cryptography technique has received attention in recent years. The encryption methods enable security of data by converting it into more complex form. Besides security, the database and communication problems are critical problems due to large data size and complexity. It has become important to reduce the size of the data by preserving the complexity.

Image Encryption using FFT with Single random matrix

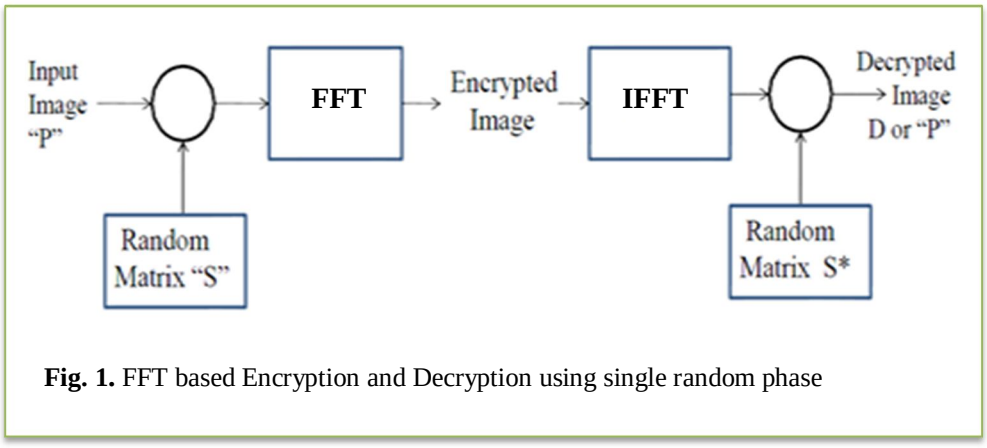

Fig. 1. FFT based Encryption and Decryption using single random phase

Fig. 1 shows the Encryption approach using single random phase method. Let an image multiplied by a single random matrix $\exp[i\phi_1(x,y)]$ and further taking Fourier transform of the result to get an encrypted image.

Decryption process is reversed by taking the complex conjugate of the random phase and further its inverse Fourier transform. Here the key is formed by the combination of the transform and the random matrix.

Approach

Double random phase encoding technique involves the use of two 2-D random phase masks. Let $h(x, y)$ indicates the image to be hidden and $g(x, y)$ denotes the encrypted image. $\exp[i\phi_{1,2}(x, y)]$ stands for the random phase masks 1 & 2 represented as the key values. The encryption process can be expressed as:

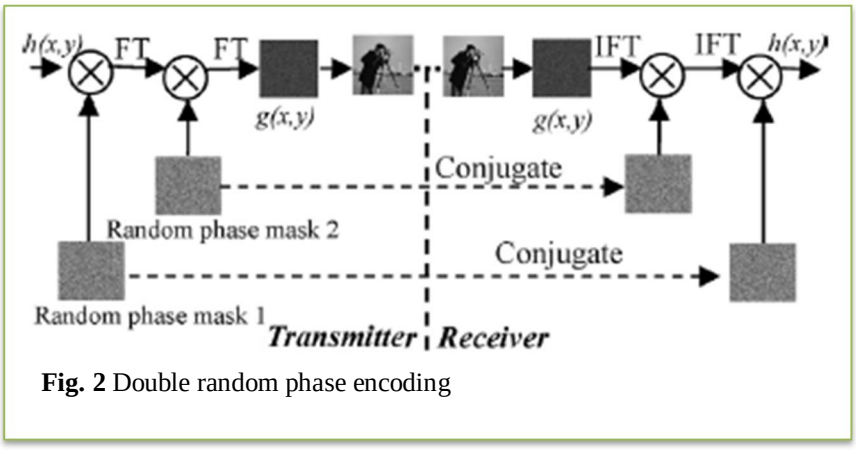

Fig. 2 Double random phase encoding

$$g(x, y) = FT\left\{FT\left[h(x, y)\exp[i\phi_1(x, y)]\right]\exp[i\phi_2(x, y)]\right\} \quad (1)$$

Then the encrypted image is dispersed and embedded into a host image to form a combined image. The corresponding decryption process is:

$$h(x, y) = FT^{-1}\left\{FT^{-1}\left[g(x, y)\exp[-i\phi_2(x, y)]\right]\exp[-i\phi_2(x, y)]\right\} \quad (2)$$

Compressive Sensing

CS is based on the recent understanding that a small collection of measurements of a compressible signal contain enough information for reconstruction and processing.

$$y = \Phi f = \Phi\Psi\tilde{x} \quad (3)$$

Where the sensing matrix Φ is a $M \times N$ matrix, where $M \ll N$. So, y becomes a $M \times 1$, while f is $N \times 1$.

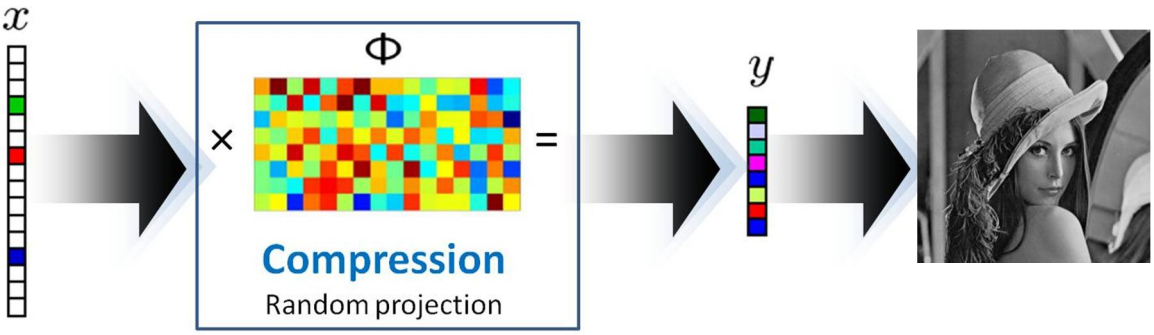

Fig. 3 Compressive sensing model shows the dimension reduction and the compression after sampling process

Digital image information encryption scheme using CS Scheme

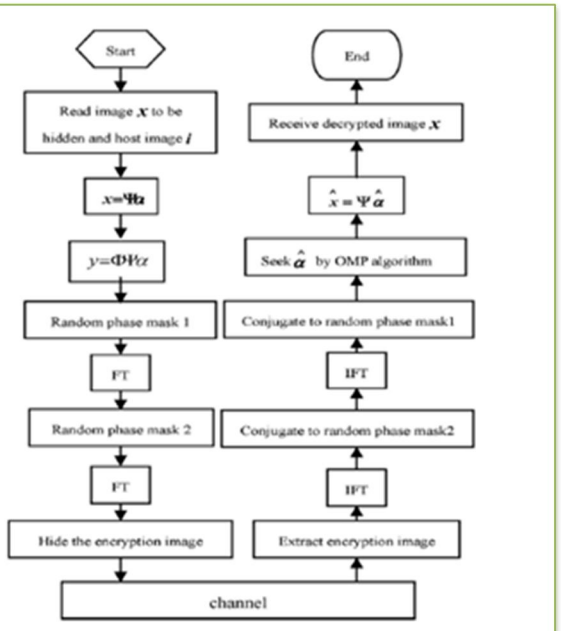

Fig. 4 Flow diagram of image information encryption and decryption

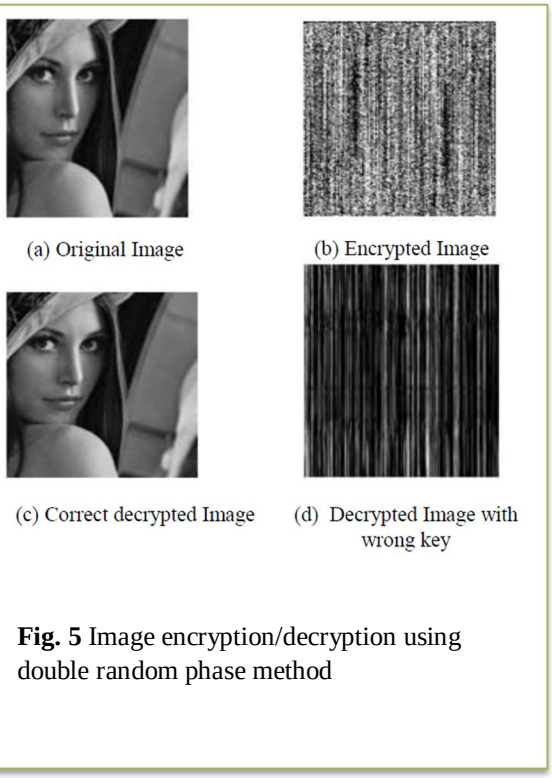

Fig. 5 Image encryption/decryption using double random phase method

In this method, the image information to be hidden is encrypted by CS firstly and the size of sampled information is reduced compared with original image.

Then, it is re-encrypted by DRPE technique where the scales of random-phase masks are also reduced correspondingly. The double-encrypted information is dispersed and embedded into the host image then transmitted through a channel. At the received terminal, original image information is reconstructed approximately via OMP algorithm after the decryption of double random-phase encoding. For CS, in order to recover the signal, the matrix A^{CS} should be available to the receiver otherwise, the gathered samples appear useless to anyone eavesdropping on the channel. This encryption comes naturally and requires no additional cost.

Simulation result

Considering natural images tend to be compressible in the transform domain, here Ψ is designed a $N \times N(N = 256)$, 2-D wavelet transform matrix which have the same size with image x to be hidden, Φ is a $M \times N$ random measurement matrix and the measuring length $M = 192$ is less than N (the value of M changes with the signal sparsity of hiding image).

Peak-to-peak Signal-to-Noise Ratio (PSNR) is used for measuring the quality of decrypted digital image as described in following equation

$$\text{PSNR}= 10\log\frac{255^2}{(1/NN)\sum_{i=1}^{N}\sum_{j=1}^{M}[R(i,j)-I(i,j)]^2} \quad (4)$$

where $R(i,j)$ is the reconstructed image and $I(i,j)$ is the initial image. The experimental result shows that the quality of decrypted digital image is very well and the PSNR is 30.8874 dB.

Wrong Key

Fig. 6 shows that when the keys of random-phase mask cannot be deciphered correctly, people who intercept information illegally cannot reconstruct original image, the security of information is ensured. It shows the decrypted image obtained after using the right key and random phase matrix. For hacker, it would be extremely difficult to acquire the correct key because one needs to know the random phase mask and the key.

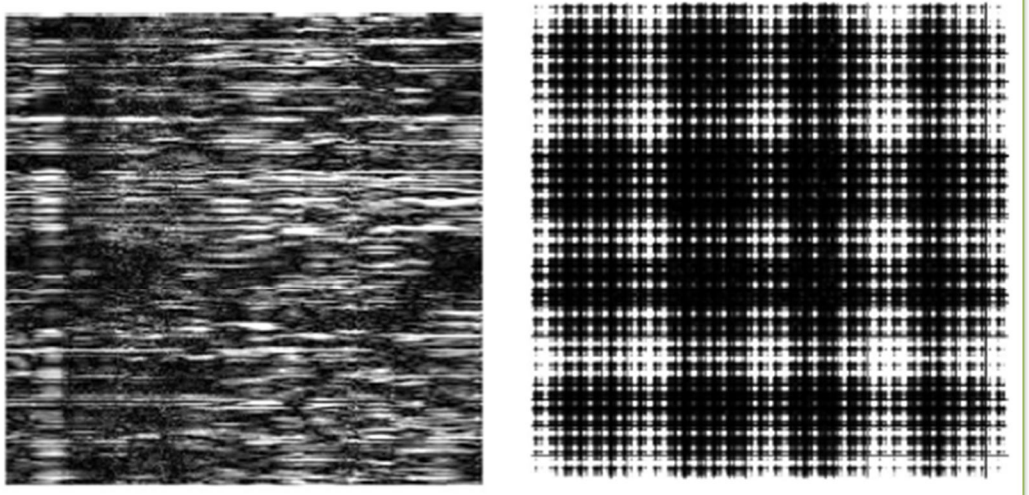

Fig.6. (a & b) Reconstructed image with a condition of wrong measurement

Conclusion

In this paper, they utilized the characteristics of CS, signal sparsity , dimensional reduction and random projection, to sample or encrypt a digital image. Then, the transformed image information can be re-encrypted by DRPE technique. In order to improve information security effectively, the image information is encrypted twice with low data volume transmission.