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

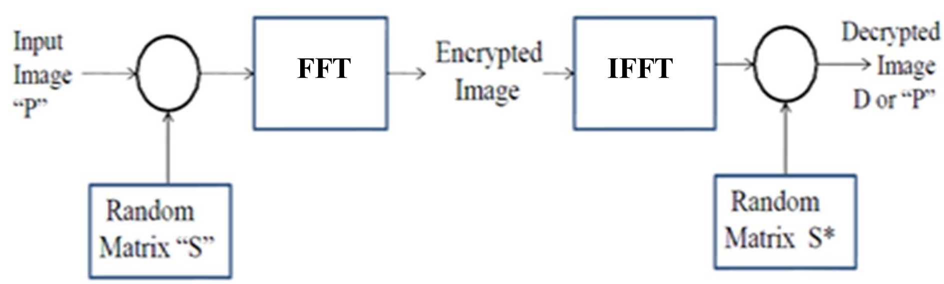


Fig. 1. FFT based Encryption and Decryption using single random phase

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:

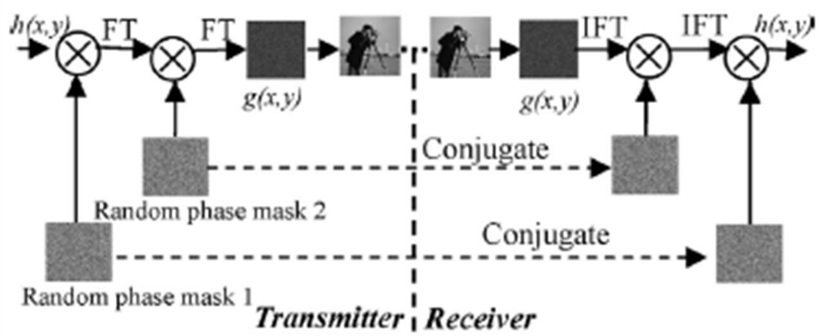


Fig. 2 Double random phase encoding

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

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

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

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 $N \times 1$.

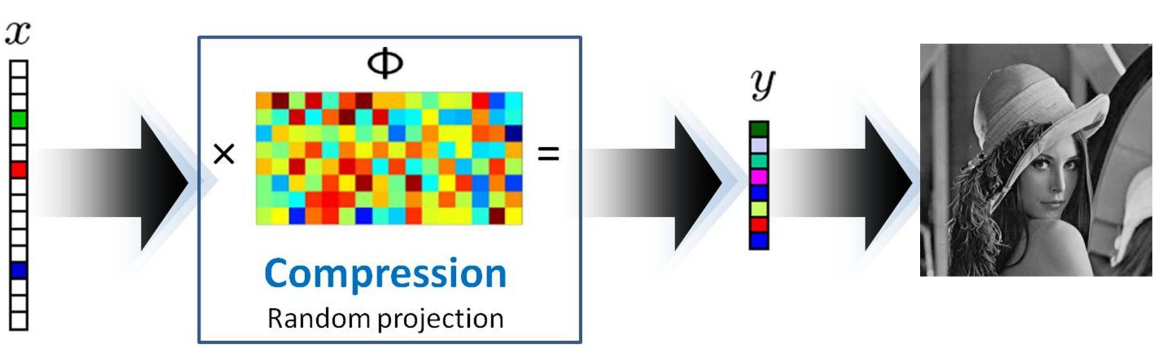


Fig. 3 Compressive sensing model shows the dimension reduction and the compression after sampling process

Digital image information encryption scheme using CS Scheme

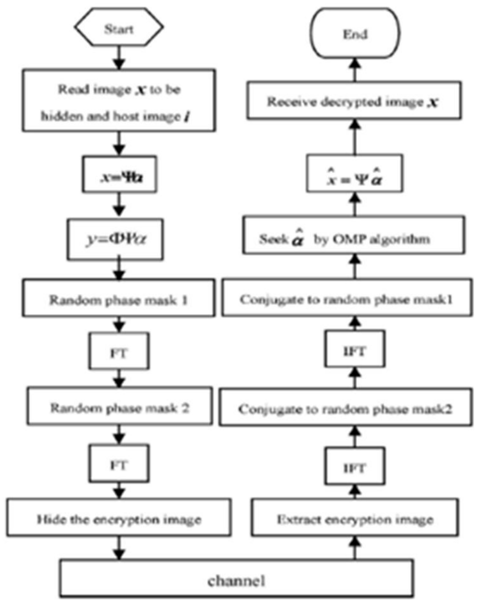


Fig. 4 Flow diagram of image information encryption and decryption

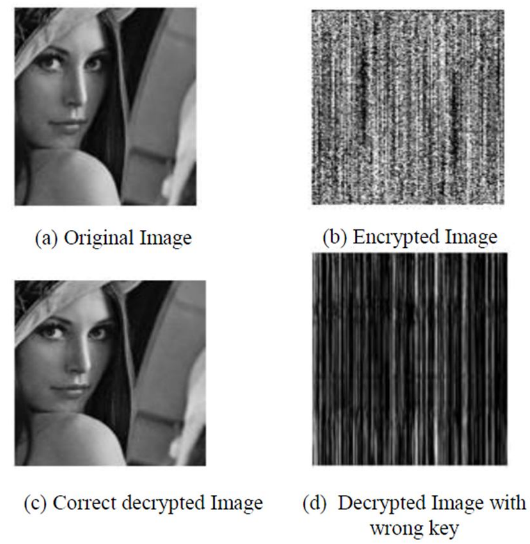


Fig. 5 Image encryption/decryption using double random phase method

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

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

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.

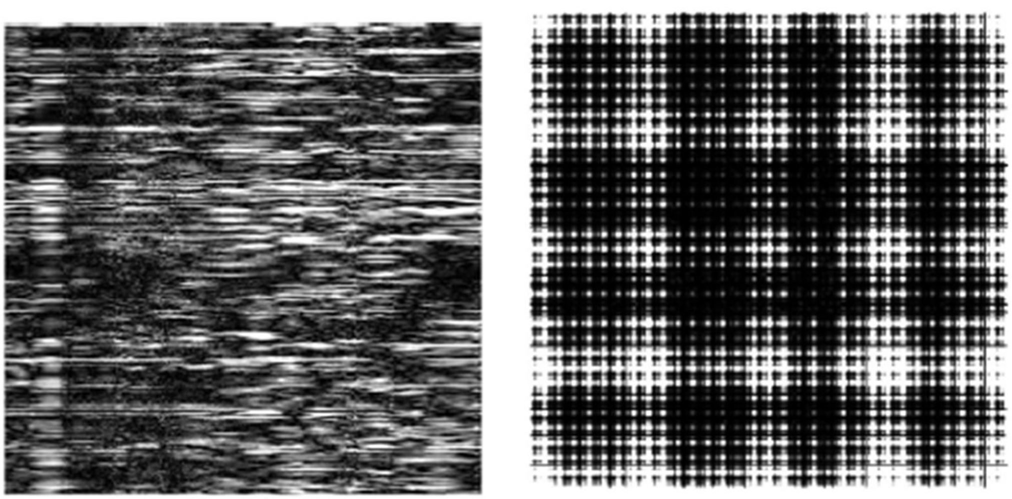


Fig.6. (a & b) Reconstructed image with a condition of wrong measurement

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.

Sparsity driven ultrasound imaging

A. Tuysuzoglu et al.

J. Acoustical Society of America (Feb. 2012.)

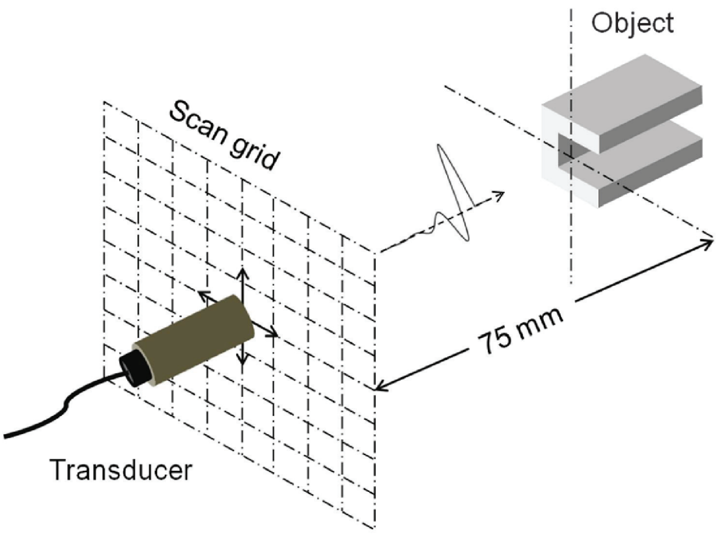
Presenter : Jin-Taek Seong

GIST, Dept. of Information and Communications, INFONET Lab.

Gwangju Institute of Science and Technology

Overview of Scenarios

- A broadband single-element unfocused transducer performs a raster scan in a plane parallel to the cross section of the object.
- At each scan position, the transducer sends an acoustic pulse and then detects the echo.
- For all experiments, the initial distance between the object and transducer was set to be 75 mm.



Introduction

- A new model-based framework for ultrasound imaging that estimates a complex-valued reflectivity field is presented.
- The benefits are:
  - Providing improved resolution and reduced diffraction artifacts.
  - Overcoming challenging observation scenarios involving sparse and reduced apertures.
- The framework is based on a regularized reconstruction of the underlying reflectivity field using a wave-based linear model of the ultrasound observation process.
- The physical model is coupled with nonquadratic regularization functions, exploiting prior knowledge that the underlying field should be sparse.
- These nonquadratic functions enable the preservation of strong physical features, i.e., strong scatterers or boundaries.

Observation model for ultrasound scattering

- The free space Green's function is used to model the scattered field in space in response to a point source of excitation,

$$G(|\mathbf{r}' - \mathbf{r}|) = \frac{\exp(jk(|\mathbf{r}' - \mathbf{r}|))}{4\pi|\mathbf{r}' - \mathbf{r}|}$$

- This can linearize the Lippmann–Schwinger equation using Born approximation to obtain the following observation model:

$$y(\mathbf{r}') = c\int G^2(|\mathbf{r}' - \mathbf{r}|)f(\mathbf{r})\, dr$$

  - where **y**(·) denotes the observed data, **f**(·) denotes the unknown complex-valued reflectivity fields
  - Note that squaring the Green's function captures the two-way travel from the transducer to the target and back

Observation model for ultrasound scattering

- The model is discretized and the presence of measurement noise is taken to be additive to obtain the following discrete observation model:

$$\mathbf{y} = \mathbf{T}\mathbf{f} + \mathbf{n}$$

  – where **y** and **n** denote the measured data and the noise, respectively, at all transducer positions; **f** denotes the sampled unknown reflectivity field; and **T** is a matrix representing the discretized version of the observation kernel.

- Given the noisy observation model, the imaging problem is to find an estimate of **f** based on the measured data **y.**

Journal Club Meeting, Sep. 24, 2013

Sparsity-driven ultrasound imaging-Imaging problem formulation

- The conventional ultrasound imaging method of synthetic aperture focusing technique (SAFT) essentially corresponds to using $\mathbf{T}^H$ to reconstruct the underlying field **f**,

$$\hat{\mathbf{f}}_{\mathrm{SAFT}} = \mathbf{T}^H \mathbf{y}$$

- The proposed method produces an image as the solution of the following optimization problem, which will be called sparsity-driven ultrasound imaging (SDUI):

$$\hat{\mathbf{f}}_{\mathrm{SDUI}} = \underset{f}{\operatorname{argmin}} J(\mathbf{f})$$

  – where the objective function has the following form:

$$J(\mathbf{f}) = ||\mathbf{y} - \mathbf{T}\mathbf{f}||_2^2 + \lambda_1 ||\mathbf{f}||_p^p + \lambda_2 ||\mathbf{D}|\mathbf{f}|||_p^p$$

  – **D** is a discrete approximation to the derivative operator or gradient, λ_1, λ_2 are scalar parameters

Sparsity-driven ultrasound imaging-Solution of the optimization problem (1/2)

- The following smooth approximation is used as

$$||\mathbf{z}||_p^p \approx \sum_{i=1}^{K} \left(\left| (\mathbf{z})_i \right|^2 + \epsilon \right)^{p/2}$$

- Using the approximation, we obtain a modified cost function,

$$J_m(\mathbf{f}) = ||\mathbf{y} - \mathbf{T}\mathbf{f}||_2^2 + \lambda_1 \sum_{i=1}^{N} \left(\left| (\mathbf{f})_i \right|^2 + \epsilon \right)^{p/2} + \lambda_2 \sum_{i=1}^{M} \left(\left| (\mathbf{D}|\mathbf{f}|)_i \right|^2 + \epsilon \right)^{p/2}.$$

- The quasi-Newton method is employed.
- The gradient of the cost function is expressed as

$$\nabla J_m(\mathbf{f}) = \tilde{\mathbf{H}}(\mathbf{f})\mathbf{f} - 2\mathbf{T}^H \mathbf{y}$$

Journal Club Meeting, Sep. 24, 2013

Sparsity-driven ultrasound imaging-Solution of the optimization problem (2/2)

- The Hessian is

$$\tilde{\mathbf{H}}(\mathbf{f}) \triangleq 2\mathbf{T}^H\mathbf{T} + p\lambda_1 \Lambda_1(\mathbf{f}) + p\lambda_2 \Phi^H(\mathbf{f}) \mathbf{D}^T \Lambda_2(\mathbf{f}) \mathbf{D} \Phi(\mathbf{f})$$

- They use $\tilde{\mathbf{H}}(\mathbf{f})$ as an approximation to the Hessian in the following quasi-Newton iteration:

$$\hat{\mathbf{f}}^{(n+1)} = \hat{\mathbf{f}}^{(n)} - \left[\tilde{\mathbf{H}}\left(\hat{\mathbf{f}}^{(n)}\right) \right]^{-1} \nabla J_m\left(\hat{\mathbf{f}}^{(n)}\right)$$

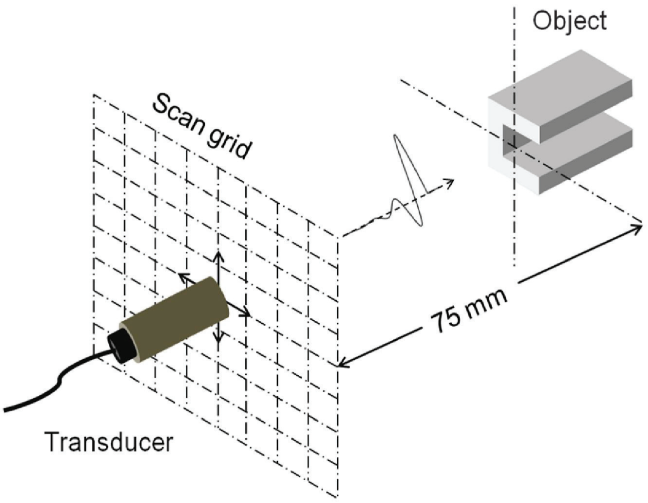
- The following fixed point iterative algorithm can be obtained:

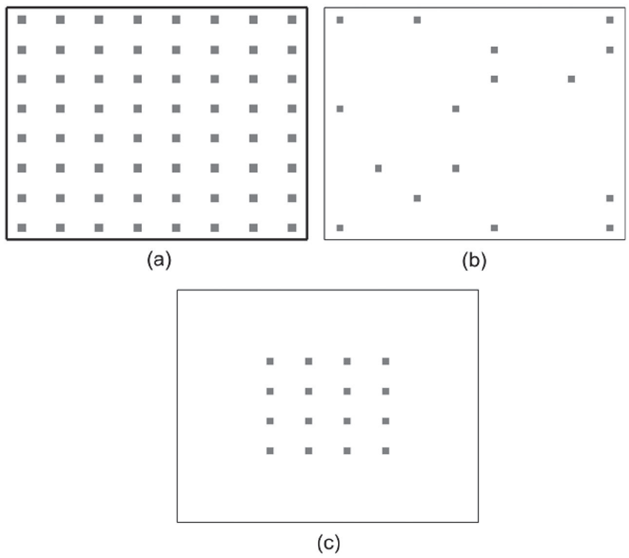
$$\tilde{\mathbf{H}}\left(\hat{\mathbf{f}}^{(n)}\right) \hat{\mathbf{f}}^{(n+1)} = 2\mathbf{T}^H \mathbf{y}$$

- The iteration runs until $\|\hat{\mathbf{f}}^{(n+1)} - \hat{\mathbf{f}}^{(n)}\|_2^2 / \|\hat{\mathbf{f}}^{(n)}\|_2^2 < \delta$

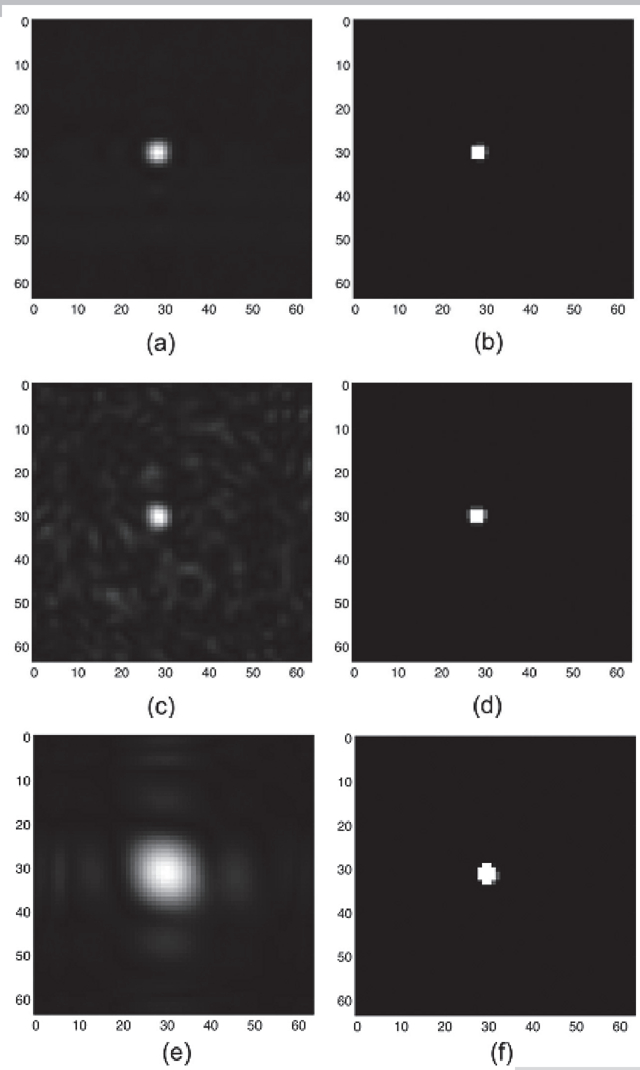
Experiments and Results

- Ultrasound experiments were carried out in a tank of water (2 X 1 X 1 m).
- Data acquisition scenarios are considered: (a) full aperture case, (b) sparse aperture case, and (c) reduced aperture case.
- A full scan forms a 64 X 64 grid with a total of 4096 scan locations.

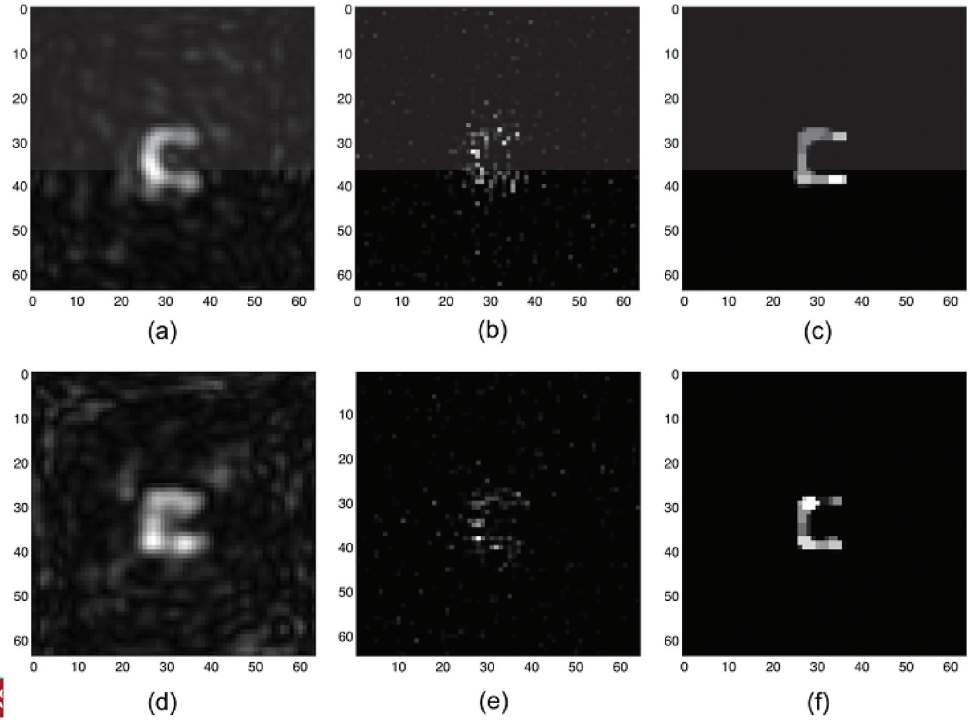




- Images of the 3.2 mm steel rod using full, sparse, and reduced aperture data
  – Reconstructions by SAFT using (a) full data, (c) 6.25% sparse data, and (e) 6.25% reduced data
  – Reconstructions by the SDUI method using (b) full data with λ_1=500, λ_2=100, (d) 6.25% sparse data with λ_1=25, λ_2=5, and (e) 6.25% reduced data λ_1=170, λ_2=5



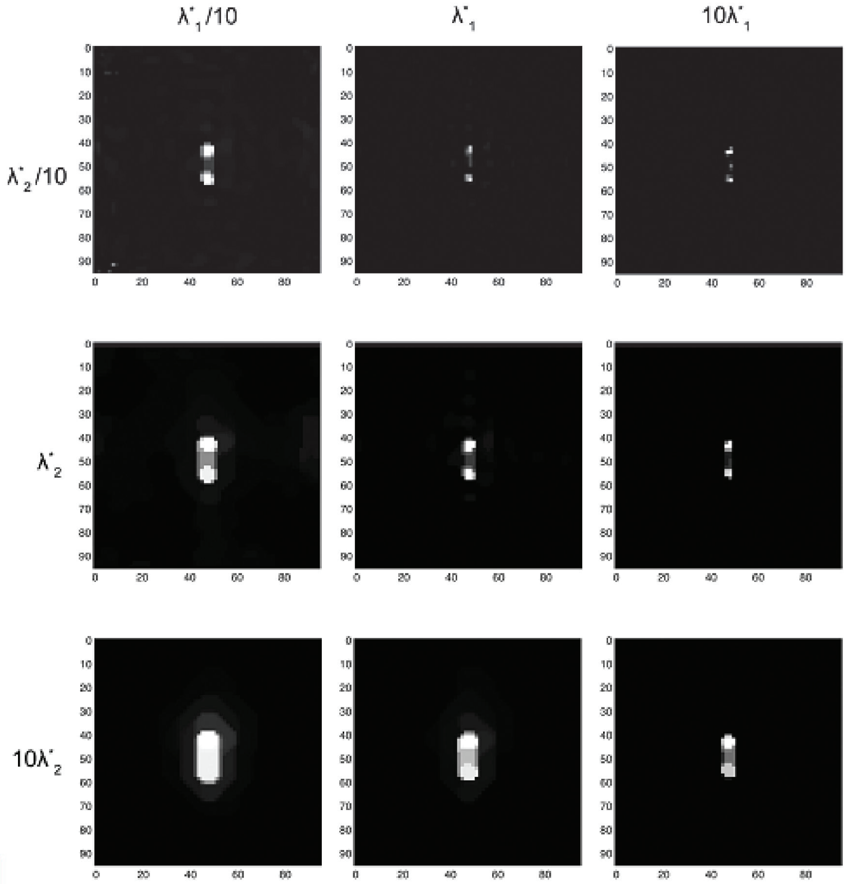
- Effect of the gradient-based regularization
  - Images of the channel using sparse aperture data. Reconstructions by SAFT using (a) 14.06% and (d) 6.25% sparse data
  - Reconstructions by the SDUI method with $\lambda_2=0$ using (b) 14.06% sparse data with $\lambda_1=20$, (e) 6.25% sparse data with $\lambda_1=5$
  - Reconstructions by the SDUI method using with (c) $\lambda_1=600$, $\lambda_2=20$ and (f) $\lambda_1=250$, $\lambda_2=10$



Selection of regularization parameters

- Recall that λ_1 scales the term that emphasizes preservation of strong scatterers, whereas λ_2 scales the gradient of the image and emphasizes smoothness and sharp transitions.
  - If the object features of interest are below the size of a nominal resolution cell, that is they should appear as "points," then they can be emphasized by choosing $\lambda_1 \gg \lambda_2$. This case leads to sparse reconstructions and can produce super-resolution.
  - If instead the object features of interest span multiple pixels, and thus form regions, these homogeneous regions can be recovered with sharp boundaries by choosing $\lambda_1 \ll \lambda_2$

- SDUI reconstructions of the 3.2 mm steel and the 3.2 mm aluminum rod separated by 10 mm reconstructed from 6.25% reduced aperture data for various choices of the regularization parameters.



Conclusions

- A new method for ultrasound image formation has been described that offers improved resolvability of fine features, suppression of artifacts, and robustness to challenging reduced data scenarios.
- The resulting nonlinear optimization problem was solved through efficient numerical algorithms exploiting the structure of the SDUI formulation.
- Results obtained from sparse aperture data scenarios suggest that SDUI can alleviate the motion artifact problem.
- The performance of the SDUI could be likely enhanced using multi-frequency data where the choice of number of frequency components and the appropriate weightings will be key factors to consider.