Study on Compressive Sensing and Image Encryption

Rajalakshmi S, M.Tech student College of Engineering Kidangoor
Anjaly Krishnan, M.Tech student College of Engineering Kidangoor

Abstract- the dimension reduction of the transmitted signal is very essential as the traffic in data transfer is increasing. Most accurate and simplest way to achieve this is by compressive sensing which means to sample a signal at much lower rate than nyquist rate. Security of the data transferred is also a very important parameter. So compressive sensing is associated with image encryption. There are many existing techniques for encrypting the compressed signal. In this paper a comparison is drawn between different sensing matrices used and also different reconstruction algorithms.

I.INTRODUCTION

Compressive sensing is a signal processing technique for acquiring and reconstructing a signal efficiently by finding solutions to underdetermined linear systems. It is a method usually used for the dimensional reduction of signal [1] [2]. This technique can be used for ensuring security to the transmitted signal. Security and privacy are of almost importance in data transmission especially in transmitting data that contains important information such as medical records and military datas.

Over the few years with the development in the field of compressive sensing the transmission of data at a lower sample rate than nyquist rate is becoming a reality. The recent researches in this area show that ensuring security along with fewer samples of data is possible [3] . In order to reduce the size of the data that has been encrypted the compression of the signal is being done first. This process requires tedious and complex computations which can adversely affect the battery life in the case of data transmission in embedded systems. So we must develop a technique where encryption and compression has to be done simultaneously.

Through this paper we would like to compare the different encryption techniques that have been used in compressive sensing based image encryption. Many improvements are happening in the field of compressive sensing .Recent researchers have developed techniques for encryption and compression at same time using much simpler computations.

COMPARISON OF SENSING MATRIX

Random Matrix

The encryption and compression of the data that has to be transmitted is only possible by projection of the signal on to sensing matrix. As the projection the reconstruction of the projected signal is also essential [4] [5]. In compressive sensing sampling process is replaced by sensing matrix.

One of the initial sensing matrix that was being used for the projection of the signal was the random matrix. In this technique the matrix is chosen in random. Here we map a set of p points into O(log(p)) dimensions without disturbing the inter point distances. Fig 1 shows the conventional compressive sampling using random matrix.

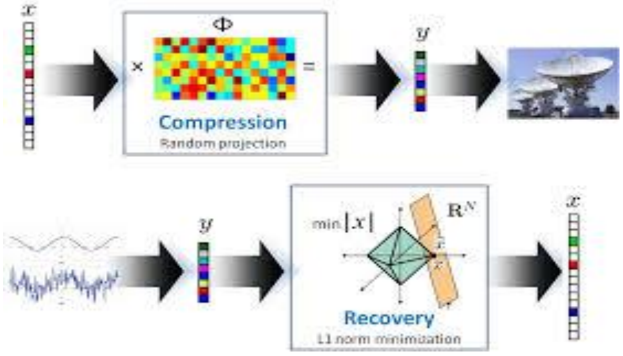


Fig1: *compressive sensing using random matrix*

Elementary approach in random matrix is mainly based on the same concentration inequalities for random inner products. The ensemble Φ is created by drawing each element independently from a sub gaussian distribution.

$y_k = <\phi_k, x_0>$, k = 1, . . . , m (1.1)

where x_0 is the transmitted signal which is having sparsity and y_k represents the inner product of the signals.

Next important approach is random sampling from an incoherent orthobasis. In this scenario measurement waveforms ϕ_k are selected from rows of an orthogonal matrix $\Phi^{'}$.When we randomly sample from a fixed orthosystem $\Phi^{'}$, the number of samples required to reconstruct the signal depends on the relationship between $\Phi^{'}$ and Ψ. One of the ways to quantify this relationship is by using mutual coherence.

Very recent improvement in random sensing matrix is the introduction of Random convolution. In this the measurement process has the following two steps:

1. Circularly convolve the signal x_0 € R^n with a pulse h € R^n. The pulse is random, global, and broadband such that its energy is distributed uniformly across the discrete spectrum.

2. Compressing the signal by sub sampling using different methods.

.

B.Optimized Matrix

Many modifications to the random matrix technique lead to the discovery of optimized sensing matrix. Optimized sensing matrix considers the projection of a matrix Φ for a compressive sensing system for which the dictionary ψ is being given unlike in the case of random matrix. The optimal projection matrix is designed in terms of finding those Φ such that the Frobenius norm of the difference between the Gram matrix of the dictionary ΦΨ and the identity matrix is minimized. With the generalization of the previous experiments a class of solution is derived in closed manner. The solution set is characterized by an arbitrary orthonormal matrix. Experiment results shows that the projection matrix obtained by this approach significantly improves the signal recovery accuracy of the CS system and outperforms those by existing algorithms.

A small mutual coherence between the measurement matrix and the representing matrix is a requirement for achieving a successful CS. The mutual coherence parameter of equivalent
dictionary was defined in [5] as

$$\mu(D) = \max_{i\neq j, 1\leq i,, j\leq k}\{d_i^T d\} \qquad (2.1)$$

In order to minimize μ(D) the gram matrix of D is designed close to the identity matrix I and the optimized matrix can be written as

$$D = \arg\min \|D^T D - I\|^2 \qquad (2.2)$$

The optimized sensing matrix technique is classified into different categories. The first among them is by using the Elad's method. In [8], Elad minimized the averaged mutual coherence to optimize the sensing matrix. Here instead of using averaged matrix Elad used difference coherence *t*- averaged mutual coherence which reflects the average behavior. The main objective of this method is the reduction of the absolute inner products which are above *t* [6]. The Gram matrix of the normalized equivalent dictionary is computed and the values above *t* are compressed by multiplying with γ ($0 < \gamma < 1$).Many iterations are done to get accurate results.

Another method is called the Sapiro's method wherein unlike the previous method it is non-iterative. Instead of targeting on *t*-averaged mutual coherence between **Φ** and **Ψ**, this method makes any subset of columns in **D** as orthogonal as possible, or equivalently, making the Gram matrix as close as possible to an identity matrix I.

Elad's method is time-consuming and the shrinkage function creates large values that are not present in the original Gram matrix. Large off diagonal values in the Gram matrix ruin completely the reconstruction algorithms. Sapiro's method is non-iterative and the reconstruction relative error rate is high. To overcome this novel method based on ETF is proposed. The objective is to find an equivalent dictionary which is close to an ETF because of the minimum coherence property of ETF, and then from the equivalent dictionary, the optimized projection matrix is being constructed. Many modifications were added to these techniques one among them is to use *G* □□D^tD *(2.3)*
and using it as initial Gram matrix instead of using G. This technique is called as MC-ETF[7] [8].

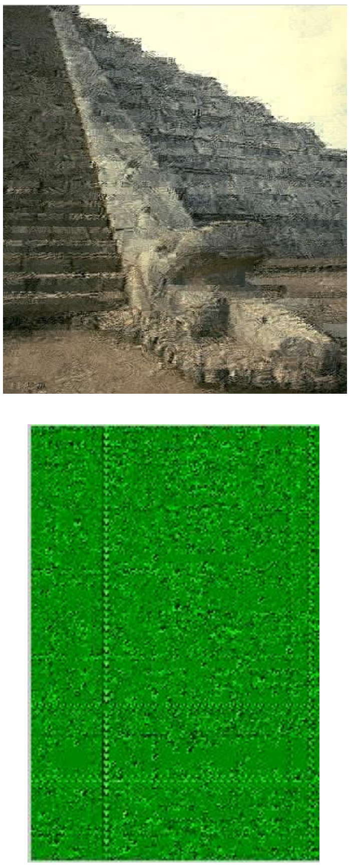


Figure 2:Test image and the Encrypted image

.

.

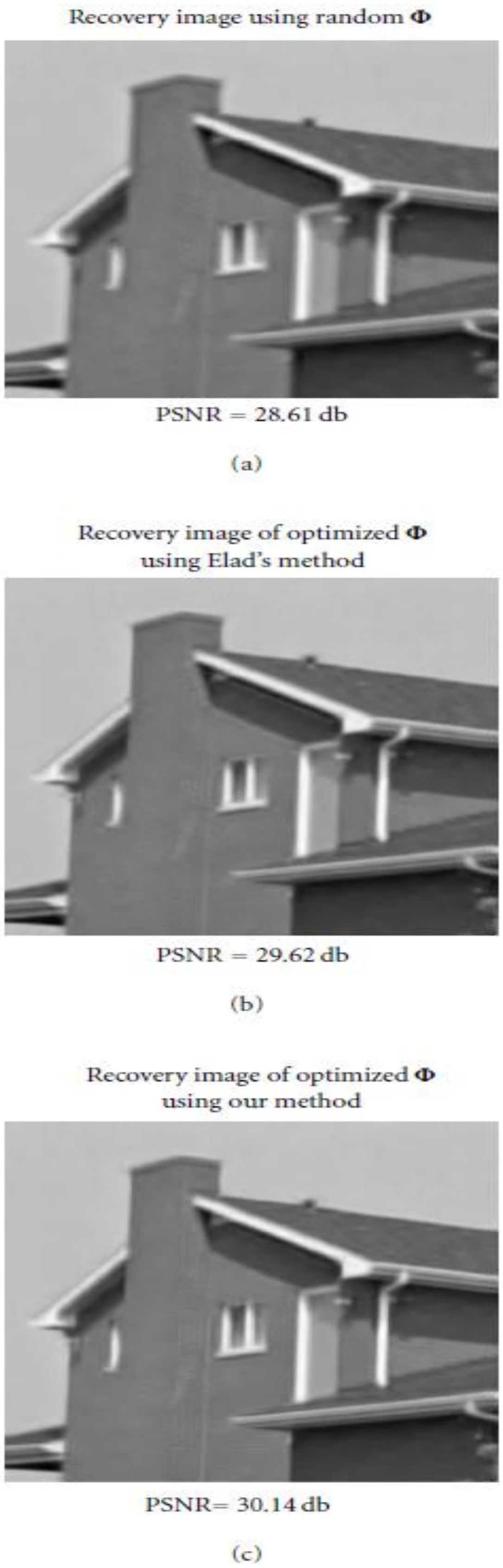

Recovery image using random Φ
PSNR = 28.61 db
(a)
Recovery image of optimized Φ using Elad's method
PSNR = 29.62 db
(b)
Recovery image of optimized Φ using our method
PSNR= 30.14 db
(c)

Figure 3:Image obtained for different matrices[9]

III.COMPARISON OF RECONSTRUCTION TECHNIQUES

Reconstruction of the projected signal is also very important for efficient transfer of data. Many specialized reconstruction techniques are in use today. Primarily simple basis functions were used for signal reconstruction. Later on a method called Matching pursuit algorithm was used. Matching pursuit (MP) is a sparse approximation algorithm which involves finding the best matching projections of multidimensional data onto the span of a redundant dictionary. As an extension to this orthogonal matching pursuit (OMP) was introduced. The main difference from MP is that after every step, *all* the coefficients extracted so far are updated, by computing the orthogonal projection of the signal onto the set selected so far [9]. This can lead to better results than standard MP, but requires more difficult computation.

Another method is stage wise gradient pursuit. Here several elements are selected during each iterations which makes it a possible solution to the computation of large problems. The selection is done in step by step manner.

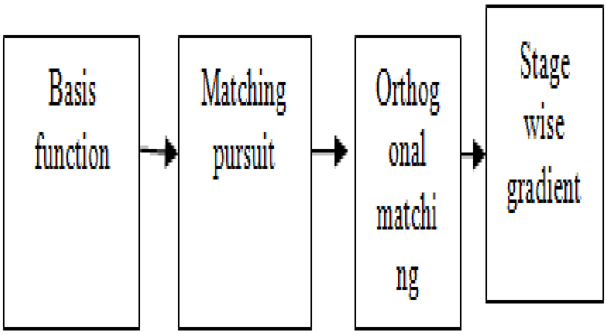
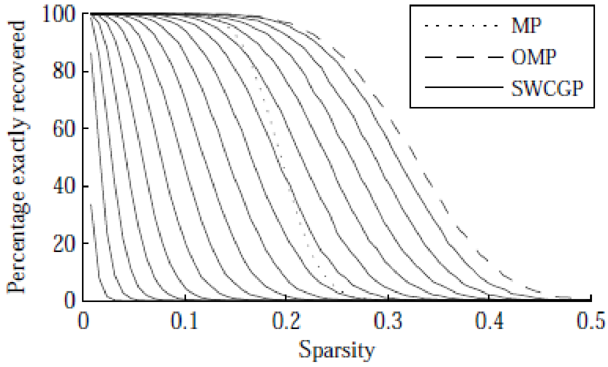


Figure 4: Evolution of reconstruction algorithms



.Figure 5: Comparison of different reconstruction algorithms MP, OMP and Stage wise gradient [10]

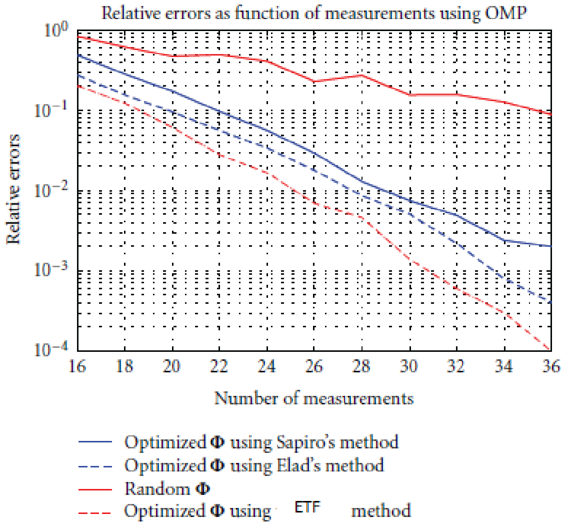


Figure 6: Errors in OMP as function of number of measurements

IV.CONCLUSION

Through these comparisons we concluded that with using Modified ECF the computation difficulty can be reduced and the efficiency of sensing matrix gets improved. For reconstruction techniques stage wise gradient pursuit is the best algorithm for accurate reconstruction of the encrypted signal at the receiver.

ACKNOWLEDGEMENT

We would like to thank the funding provided by 'TEQIP phase III' of College of Engieering Kidangoor for the publishing of this paper

REFERENCES

[1] David L. Donoho, Compressed Sensing, IEEE Transactions on Information Theory., vol. 52, no. 4, pp. 1289-1306, Apr. 2006

[2] Emmanuel J. Candès, Justin Romberg, and Terence Tao, Robust Uncertainty Principles: Exact Signal Reconstruction From Highly Incomplete Frequency Information, IEEE Transactions on InformationTheory., vol. 52, no. 2, pp. 489-509, Feb. 2006

[3] E. Candès, J. Romberg, and T. Tao, Stable signal recovery from incomplete and inaccurate measurements, Comm. Pure Appl.Math.,vol. 59, no. 8, pp. 1207–1223, Aug. 2006

[4] Emmanuel J. Candès and Terence Tao, Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies?, IEEE Transactions on Information Theory., vol. 52, no. 12, pp. 5406-5425,Dec. 2006.

[5] M. F. Duarte and Y. C. Eldar, Structured compressed sensing: from theory to applications, IEEE

[6] M. Elad, Dec., Optimized projections for compressed sensing, IEEE Transactions on Signal Processing, vol. 55, no. 12, pp.5695–5702, 2007

[7] Jianping Xu, Yiming Pi and Zongjie Cao,Optimized Projection Matrix for Compressive Sensing, EURASIP Journal on Advances Signal Processing, vol. 2010, Article ID 560349, 8 page doi:10.1155/2010/560349, 2010