Study the Effects of Encryption on Compressive Sensed Data

Minal N. Chavhan, S.O.Rajankar

Abstract - Today's technological era is highly dominated by data transfer. Since confidential data is transmitted over risky media like internet, faithful data transfer is now accompanied with secure data transfer. Security is the need of the hour. Here, a new and relatively simple encryption algorithm is proposed which shuffles the elements. It randomizes the data. But this algorithm is applied on compressed sensed data which inherently has encryption properties. A study of the security of this additional encryption algorithm over the compressed sensed data is done and observed the objective quality of the recovered data in presence of noise.

Index Terms- compressive sensing, faithful data transfer, objective quality, security

I. INTRODUCTION

With the extensive usage of internet which is unreliable communication network, cryptographyprovides a secure way of information security. It is an effective way for protecting the sensitive data that is stored on media devices or transmitted over an unsecured network communication path by encrypting i.e. converting into an unreadable format i.e. cipher-text. Typically, encryption of the multimedia is performed following the compression. This paper introduces a novel way of combining encryption and compression.A variety of encryption algorithms have been introduced in last few years. Bani-Younes and Jantan [1] introduced a block-based transformation Algorithm based on the combination of image transformation and the well-known Blowfish encryption and decryption Algorithm. Krikoret al. [2] proposed a method for image encryption which selects some DCT high frequencies that are taken as the characteristic values. The resulting encrypted blocks are shuffled according to a pseudo-random bit sequence. Shuffle Encryption Algorithm (SEA) is proposed in [3] that applies nonlinear byte substitution. An AES based encryption algorithm is proposed in [4].

Compressed sensing (CS) framework proposed in [5], provides a unique way of unifying sampling and compression. It reduces the data acquisition and computational load at sensors, at the cost of increased computation at the intended receiver. Compressive sampling relies on the sparseness of the signal and gathers linear measurements $y = Ax$ of a sparse signal x, where size of y is a small fraction of the samples needed for Nyquist sampling. A is the lineartransform which carries certain regularities. The receiver obtains thelinear measurements$y$ and reconstructs the image by solving an optimization problem.

Manuscript received on June, 2013

Minal N. Chavhan, E&TC dept.,Sinhgad college of Engg. Pune University, India.

S.O.Rajankar, E&TC dept.,Sinhgad college of Engg. Pune University, India.

Compressed sensing also provides good encryption properties. The measurements y are a function of sensing matrix A. Since the receiver has to know this information in order to formulate the optimization problem and to reconstruct the signal, the CS measurements can be considered as an encrypted representation of the original signal. The security of the encryption method relies on the fact that the sensing matrix A is not known to an attacker [6]. The attacker first has to decrypt the data and then determine the matrix A.

In this paper, we are going to study the effect of using an additional encryption algorithm on the security and objective quality of compressed sensed data. Here, the data taken is 32x32 and 54x54 monochrome and colour images. First, the images will be compressed sensed and we will have CS measurements y. The encryption algorithm is applied on these measurements. The algorithm involves simple row and column rotation followed by shuffling of the elements. Then the sign of the elements are made opposite. This algorithm will additionally make the matrix random which inherently has cryptographic properties. An attacker has to first break the security of this algorithm and then try guessing the measurement matrix to recover the original signal. After decryption, the CS measurements will be recovered by using total variation minimization method. Results will include the objective quality assessment of the recovered image and examine security of encryption algorithm on CS data.

The paper is organized as follows: Section 2 gives a brief idea of compressive sensing. Encryption algorithm is introduced in Section 3. Section 4 explains the encryption of the key. Section 5 gives the results depicting faithful reconstruction and objective quality of image after applying the encryption algorithm on CS measurements.

II. COMPRESSIVE SENSING

Compressive sensing (CS) is anunifying framework for signal acquisition and compression. CS reduces the number of measurements required to completely describe a signal by exploiting itscompressibility. The concept is based on the work of Candes, Romberg, and Tao [7]and Donoho [8], who showed that if a signal has a sparse representation in a certain domain then it can be recovered with only a few samples of its projection in a second domain which is incoherent with the sparse (first) domain. The recovery relies on accurate prediction of the K basis functions over which the signal is sparse. The aim is to recover the signal length N and the sparsity K where K << N, from the few sample measurements M of the second basis set. The M measurements can be transmitted over transmission channels with little or no modification. Another fact to note is that independent and identically distributed Gaussian or Bernoulli basis functions are incoherent with all other basis functions thus we can make generalized CS encoders which

could work with many different types of signals irrespective of the domains in which they are individually sparse. Compressive Sensing maps a signal from higher dimension (N) to significantly lower dimension (M). The compressively sensed samples can be represented as

$y = \varphi\psi\alpha$

i.e. $y = \Theta\alpha$ …(1)

where $\Theta = \psi\varphi$,

φ is the sensing matrix,

ψ is the incoherent transform basis.

Here α is a K sparse vector, y is the measurement vector. Sparse Basis (ψ) is a transform basis over which the signal to be transmitted (x) becomes sparse. Example for an image signal, ψ could be DCT or wavelet transform. Projection Basis (φ) or the sensing matrix is the second basis set which is incoherent with ψ and is used to extract some selected samples of the signal which would be transmitted over the channel. Incoherent projections (y) are the CS sampled versions of x which are transmitted over the channel after appropriate channel encoding. $\Theta = \psi\varphi$ is the product transform. From its definition we can say that y is K-sparse over Θ.

A necessary and sufficient condition for stable recovery of original signal x from CS measurements is that the measurement matrix Θ must have restricted isometry property (RIP). An alternative approach to stability is to ensure that the measurement matrix φ is incoherent with the sparsifying basis in the sense that the vectors $\{\alpha_j\}$ cannot sparsely represent the vectors $\{\psi_i\}$ and vice versa [8]-[10].

To recover the signal x, recovery algorithms are proposed in [7]. Most popular are the *l-norms*. l_1 recovery can be formulated as,

$\min \|x\|_1$ s.t. $y = Ax$. …(2)

Sometimes when the data is natural image, these algorithms produce ringing artifacts. To overcome this, we can solve a slightly different optimization problem to recover the image from the same corrupted measurements [5]. If $y = x_0 + e$ is a "noisy" observation of an image x_0, we restore x_0 by solving

$$\min_x \mathrm{TV}(x) \text{ subject to } ||x - y||_2^2 \le \epsilon^2 \quad \ldots(3)$$

$$\mathrm{TV}(x) = \sum_{i,j} ||D_{ij}x||_2, \; D_{ij}x = \begin{bmatrix} x(i+1,j) - x(i,j) \\ x(i,j+1) - x(i,j) \end{bmatrix} \quad \ldots(4)$$

where ϵ should be something close to the expected size of $\|e\|_2$. The total variation of the image x is the sum of the magnitudes of the gradient. It tends to remove the noise in the image while retaining the sharpness of the edges, and the recovery does not suffer from the "ringing artifacts" to which wavelet methods are prone.

III. ENCRYPTION ALGORITHM

The proposed encryption algorithm applied on CS measurements is a one which will simply rotate rows and columns. The obtained matrix y will be divided into 4×4 blocks. Second step is that rows are rotated downwards by 1 and columns are rotated to right by 3. This rotation process is repeated for 3 times. Step 3 is to shuffle the outer diagonal elements i.e. f(0,0) with f(3,3) and f(0,3) with f(3,0). Step 4 is to shuffle the inner diagonal elements i.e f(1,1) with f(2,2) and f(1,3) with f(3,1). Step 5 is to again rotate rows and columns. Step 6 is to change the signs of all elements. And finally take the transpose of the matrix. This will create more random structure. To recover the original image, we need to decrypt these measurements. Decryption process is exactly the opposite. But the receiver should know that by how many times the rotation is done and for how many times the process is repeated. This rotation number can be mutually decided by both parties

IV. ENCRYPTION OF KEY

For the decryption of this algorithm, one should know the size of the matrix, size of the blocks, number of rotations of rows and columns. Therefore a key is generated explaining all of the above mentioned. But this key is also encrypted. Each element of the key is added to randomly generated number. The result is multiplied with a constant. Obviously, the randomly generated nos. must be conveyed to the receiver secretly. Without these numbers, it's very difficult to decrypt the key. Suppose the key is 13 13 5 4 4 4 5 4 2 2 1 1. The size of the matrix is 13x13. Matrix is divided into 3 rows, each of size 5, 4, 4 respectively and into 3 columns of size 4, 5, 4 respectively. Latter denotes the rows and column rotation.

V. EXPERIMENTAL RESULTS

The software used is MATLAB. For compressed sensing, l1-magic package is used which includes the convex optimization routines. Input is taken as 32x32 and 54x54 images. The DCT basis acts as the sparsifying basis(ψ). The product matrix $\Theta = \psi\varphi$ or $A = \psi\varphi$is obtained by randomly selecting rows from sparsifying basis. Also Gaussian noise is added to the product basis to observe the objective quality of the recovered data. The linear measurements y which is a column vector, are obtained by projecting the image elements on the product basis, using (5). The sparsity (K) of the image data is assumed as 300.

$M >= c*K*\log(N/K)$ …(5)

The column vector so obtained is now converted into a matrix. It is partitioned into blocks of uneven sizes. The encryption algorithm is applied on the data and again it is converted back into a column vector. Then the encrypted key is attached to it and we get our final encrypted data which can be used for reconstruction of the image. The random numbers generated for the key should be sent to the receiver privately. Here, the constant to be multiplied with the key is taken to be half of the length of the key.

For reconstruction of the image, first remove the key and decrypt it. Since, the random numbers are known, length of the key and hence the constant to be multiplied can be derived. With the key, decryption of data is done. Total variation reconstruction algorithm is applied over the data to recover the original image. It is available in L1 magic.

A. Observed Objective Quality

We have added the Gaussian white noise with zero mean and 0.01 variance to the measurement matrix Θ or A. the objective quality of the image is observed by calculating the Peak Signal to Noise Ratio (PSNR) of the corresponding perturbation level of the image. Since the image is represented in 8-bits, PSNR is given by,

$$\mathrm{PSNR} = 10 log_{10} \frac{256}{MSE} \quad \ldots(6)$$

The normalized perturbation (nPERT) level on Θ is calculated in dB as,

$$\text{nPERT}=10log_{10}\frac{||\Theta'-\Theta||_F^2}{||\Theta||_F^2}. \quad ...(7)$$

where Θ′ is Gaussian white noise added measurement matrix.

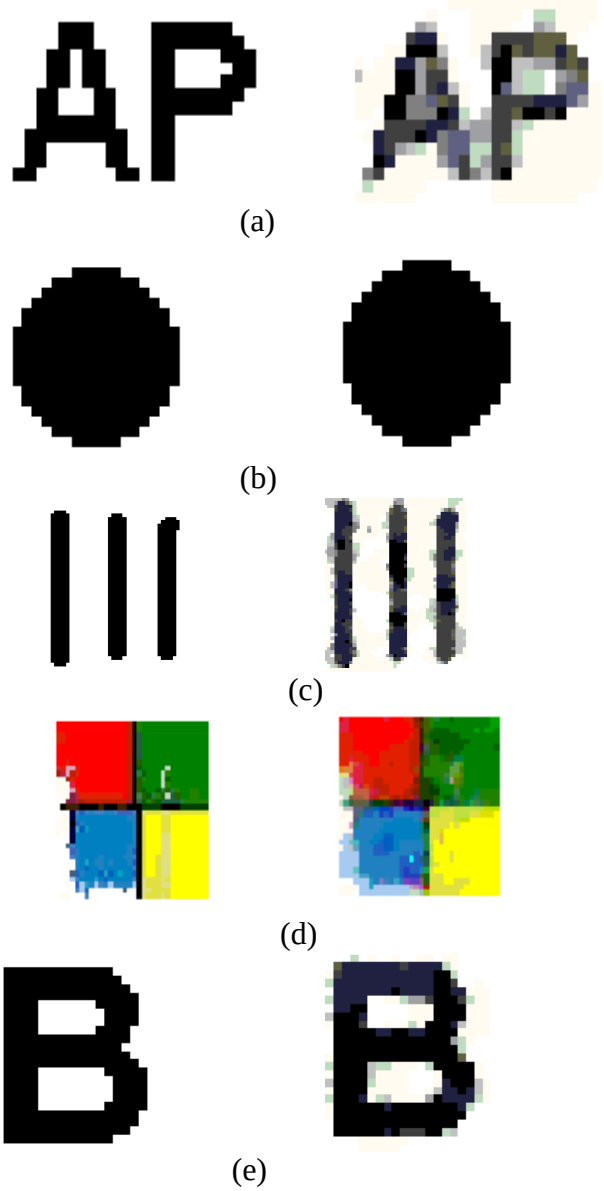

Figure 1: Original and recovered images of (a)54x54 alphabets image (b)32x32 dot image (c)54x54 lines image (d)32x32 colour square image (e)32x32 alphabet image

Table 1 Objective quality of image

IMAGES	MSE	PSNR	nPERT
1]dot-32x32	3.4755e-007	102.7546	0.2612
2]AP-54x54	0.0162	66.0593	-0.2608
3]lines-54x54	0.0151	69.8295	-0.1537
4]B-32x32	0.0045	74.0.173	-0.2622

Figure 1 shows the recovered images. It can be clearly seen that the image quality is pretty good. Above table gives us the objective quality of the images. The PSNR values are quite high with the corresponding perturbation level.

B. Security of the Encryption Algorithm

The security of the algorithm lies in the key. Suppose the key is 13 13 5 4 4 4 5 4 2 2 1 1. Length of the key is 12. Random number is added to each digit, i.e. 12 random numbers. To guess these numbers, one needs to do permutation of 12^{12}. As the length of the key increases, so do the calculations. It becomes quite impossible to guess the numbers. Also the constant which is multiplied also have to be guessed.

In order to reconstruct the image, an attacker has to first decrypt the algorithm which involves n^n permutations of the key. Other way to decrypt the algorithm is to try out various combinations of the size of matrix, then look out for the block sizes and then apply decryption algorithm. To guess the block size is not feasible since we can partition the image into n number of rows and columns to get varying sizes of blocks. After decryption of the algorithm, one needs to obtain the measurement matrix Θ to get the original data.

VI. CONCLUSION AND DISCUSSIONS

This paper examines the security of the encryption algorithm applied on the compressed sensed data and also determines the objective quality of the recovered image. We consider the complexity of the decryption of the key in section V(B). We can say that as the size of the image increases, the number of row and column partition also increases, thereby increasing the number of blocks. This in effect will increase the length of the key. Since the random numbers are equal to the length of the key, a key of length n will need to do permutation of n^n. But the size of the block is inversely proportional to the number of operations performed in the encryption algorithm. So we need to balance the security and number of operations performed per block. With the high speed computer, this would not be such a big issue.

We have used total variation minimization recovery algorithm for the recovery of the decrypted data which helps in denoising of the data. For this purpose we have added Gaussian white noise. From section V(A). we can see that the objective quality for the corresponding added noise is good.

Application of this project would be in transmission of the confidential images where only recognition of the object is important and not the overall clean image quality such as web remoting.

APPENDIX

(A) Restricted isometric property

Let A_T be a submatrix of A formed by taking any T columns of A, where $T \leq S$; with S denoting an upper bound the sparsity of the signal of interest x_0.The S-restricted isometry constant of A is then defined as the smallest value of δ_S which satisfies:

$$(1-\delta_s)\|c\|_2^2 \leq \|A_T c\|_2^2 \leq (1+\delta_s)\|c\|_2^2 \quad ...(8)$$

for all $T \leq S$ and all coefficient sequences $(c_j)\ j \in T$.

Observe that when A_T is a matrix with orthonormal columns, we get $\delta_S = 0$. Thus δ_S represents how closely the system of linear equations with coeffiecients given by A_T for $T \leq S$ behave as an orthonormal system. The matrix A satisfies the RIP if:

$$\delta_S+\delta_{2S}+\delta_{3S}<1 \quad ...(9)$$

In words, the matrix A_T must preserve the lengths of these particular S-sparse vectors.

(b) l_p norms:

Reconstruction algorithms use these norms. The l_p of a vector $\alpha \in R^n$ is defined as,

$$\|\propto\|_p := (\sum_1^N(\propto_i)^p)^{\frac{1}{p}} \quad ...(10)$$

For instance, $l_2$norm of a vector is the square of its Euclidean distance. Similarly for p=0, is the number of non-zero elements present in *x*.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm",*IAENG International Journal of Computer Science*, 35:1, IJCS_35_1_03.

[2] Krikor L., Baba S., Arif T., and Shaaban Z., "Image Encryption Using DCT and Stream Cipher", *European Journal of Scientific Research*, vol. 32, no. 1, pp. 47-57, 2009.

[3] Yahya A. and Abdalla A., "A Shuffle Image-Encryption Algorithm", *Journal of ComputerScience*, vol. 4, no.12, pp. 999-1002, 2008.

[4] Jayant Kushwaha, Bhola Nath Roy, "Secure Image Data by Double encryption", *International Journal of Computer Applications* (0975 – 8887),Volume 5– No.10, August 2010.

[5] Sanil Fulani, Dr. K.R. Rao.,"Compressive Sensing of Image and Application to Communication Channel Coding."

[6] Adem Orsdemir, H. OktayAltun, Gaurav Sharma, Mark F. Bocko, "On the Security and Robustness of Encryption via Compressed Sensing", 978-1-4244-2677-5/08/$25.00 © 2008 IEEE.

[7] Emmanuel J. Candès, Justin Romberg, Terrance Tao, "Stable Signal Recovery from Incomplete and Inaccurate Measurements," *Communications on Pure and Applied Mathematics*, Vol. LIX, 1207–1223 (2006) ©2006 Wiley Periodicals, Inc.

[8] Donoho D., "Compressed sensing", *IEEE Transactions on Information Theory*, **52**, 4 (Apr.2006), 1289—1306.

[9] Emmanuel J. Candès, Michael B. Wakin, "Compressive sampling ppt".

[10] Emmanuel J. Candès, Justin Romberg, "Robust Uncertainty Principles: Exact Signal Reconstruction From Highly Incomplete Frequency Information", *IEEE transactions on information theory*, vol. 52, no. 2, february 2006

[11] Justin Romberg, "Variational Methods for Compressive Sampling", Electrical and Computer Engineering, Georgia Tech, Atlanta, GA.

[12] Emmanuel Candes and Terence Tao, "Near Optimal Signal Recovery From Random Projections: Universal Encoding Strategies", *IEEE Trans. Inform. Theory*, submitted. Ar Xiv: math.CA/0410542,October 2004.

[13] Heung-No Lee, "Introduction to Compressed Sensing", GIST, Korea, 2011, pp 20-26, 86-95.

[14] Stephen Boyd, Lieven Vandenberghe, *Convex Optimization*, Cambraidge University Press, pp. 7-10, 21, 561-570, 609- 612.

[15] Chuong B. Do, *Convex Optimization Overview* (cnt'd), November 29, 2009