Ensuring Security to the Compressed Sensing Data Using a Steganographic Approach

A.V. Sreedhanya and K.P. Soman

Abstract--- *This paper focuses on the strength of combining cryptography and steganography methods to enhance the security of communication over an open channel. Here the data to be send are secured by using the compressive sensing method and the Singular Value Decomposition (SVD) based embedding method. The data is encrypted using the compressive measurements of the data and the resultant data is embedded in the cover object using the SVD based water mark embedding algorithm. This approach helps to send the secret data after hiding in a cover image. The compressive sensing method helps to compress and encrypt the data in a single step. The proposed system provides more security to the compressed data. This scheme significantly reduces the attacks. This method is very useful to hide the secret images. The results demonstrate that the proposed system is highly efficient and robust.*

Keywords--- *Attacks, Compressed Sensing, Decryption, Encryption, Perfect Secrecy, Security, Sparsity, Steganography, SVD.*

I. Introduction

THE security of digital multimedia such as image, video, and audio etc, transmitted over the networks has become very important now a days. These multimedia data transmitted through the network are redundant. Transmission channel is always insecure and bandwidth-constrained. So prior to the transmission, it is desirable to compress and encrypt the data. The security to the data is provided using various cryptography and steganography methods. Steganography helps to hide the existence of the information, so it is not visible to a third party. Cryptography helps to encrypt the message. Here intruder can see the encrypted message, but it is in an unintelligible form. In the proposed system, we combined both cryptography and Steganography methods into one system for getting a better confidentiality and security. Conventional approaches for sampling signals or images follow Shannon's theorem: the sampling rate must be at least twice the maximum frequency present in the signal (so-called Nyquist rate). But the compression ratio is lesser. In this paper, the compression and encryption to the data is providedby compressive sensing. Compressive sensing is a new emerging technology; it helps to compress the data in a rate higher than the conventional approach. In compressive sensing, compression and encryption is achieved by a single linear measurement step. This step is achieved by using a measurement matrix, which is generated by using a secret key. The secret key is shared between sender and receiver.

The resultant compressed measurements are in an encrypted form. In this paper, the next level of security to the compressed and encrypted data is provided with the help of steganography. This encrypted and compressed data is hidden in the plane image using SVD based embedding method. The resultant stego image is transmitted through the network. The advantage of this proposed system is that, intruder can't detect the presence of the secret image in a plain sight. So this system helps to improve the security of the compressive sensing method in an easier way. Security to the data is provided by compressive sensing method. The proposed system helps to hide the resultant data, obtained after compressive sensing. Here in the proposed system, the compressed measurements are hidden in the plane image using SVD based water mark embedding method. But in this paper instead of watermark, we are embedding the compressed measurements in the plane image without knowing its presence. The sending of an encrypted message directly through the medium increases the attention of the eavesdropper. This proposed method helps to distract the intruders from the secret data. So the proposed system helps to reduce the attacks towards the compressive sensing technique. Various experiments have been performed to evaluate the security analysis of the presented system. According to the comparative, theoretical and experimental results; we conclude that the proposed image cryptosystem is much useful to increase the security of the compressed sensing technology. It helps to keep the storage and transmission of the secret data in a secure and reliable way.

In paper [2], Y. Rachlin and D. Baron demonstrate that compressed sensing based encryption does not achieve Shannon's definition of perfect secrecy, but can provide a computational guarantee of secrecy. In paper [1], M. RamezaniMayiami and Hamid G. Bafghi proved that the compressed sensing based-encryption achieves perfect secrecy if it satisfies some conditions. Here in this paper, the proposed system achieves perfect secrecy because of the system satisfies these conditions. Section2 provides a brief information about the compressive sensing scheme. Section3 gives the theory about the SVD based image embedding and extraction method. Section4 discuss the proposed encryption and decryption scheme. Section5 discuss the results of the

A.V. Sreedhanya, Assistant Professor, IT-Department, MEA Engineering college, Perinthalmanna, Malappuram, Kerala, India. E-mail: sreedhanya1988@gmail.com

Dr. K.P.Soman, Professor, Dept of CEN, Amrita School of Engineering, Coimbatore, Tamil Nadu, India. E-mail: kp_soman@amrita.edu

DOI: 10.9756/BIJAIP.10137

proposed system for natural and medical images. Section6 discuss the Experiments, which are conducted using different cover images and secret images. Section7 discuss the quality of the proposed encryption system. Section8 provides the security analysis for the proposed system. Section9 concludes the paper.

II. Compressive Sensing Basics

The authors of the papers [3] to [15] discuss the compress sensing paradigm and the signal recovery.

A. *Sparse Representations*

Compression with encryption of the data is performed using the compressed sensing scheme. Compressed Sensing (CS) theory asserts that one can recover certain signals and images from far fewer samples or measurements than traditional methods. CS made this possible based on two principles: sparsity and incoherence. Sparsity expresses the idea that the ”information rate” of a continuous time signal may be much smaller than that suggested by its bandwidth, or a discrete-time signal depends on a number of degrees of freedom which is comparably much smaller than its (finite) length. More precisely, CS exploits the fact that many natural signals are sparse or compressible in the sense that they have concise representations when expressed in the proper basis. It is based on the idea that objects having a sparse representation in Ψ must be spread out in the domain in which they are acquired. Incoherence extends the duality between time and frequency. Incoherence says that unlike the signal of interest, the sampling/sensing waveforms have an extremely dense representation in Ψ. The coherence between the sensing basis Φ and the representation basis Ψ is

$$\mu \;\; \Phi,\Psi \;\; = \sqrt{N} \max_{1\le k,j\le N} \left|\left\langle \Phi_k, \Psi_j \right\rangle\right| \tag{1}$$

Consider a length-N, real valued signal X^N and suppose that the basis provides a K sparse representation of X. In terms of matrix notation, we have $X = \Psi f$, in which f can be well approximated using only K non-zero entries and Ψ is called as the sparse basis matrix of size $N \times N$. For images, typical choices of Ψ include the DCT or wavelet. The CS theory states that such a signal X can be reconstructed by taking only M = O(KlogN) linear, non-adaptive measurements as follows,

$$Y = \Phi X = \Phi\Psi f \tag{2}$$

A matrix $\Phi \in R^{M\times N}$ satisfies the Restricted Isometric Property (or RIP (K, δ)) of order K<M and isometric constant 0 = δ <1. We measure and encode M< N projections by using incoherent projection, $Y = \Phi X$. Where Y is a $M \times 1$ column vector, and the measurement matrix Φ is a $M \times N$ matrix.

B. *Signal Recovery via L_1 Optimization*

The L_0 norm is used for a function that only counts the number of nonzero components. If the expansion of the original signal or image as a linear combination of the selected basis functions has many zero coefficients, then it is often possible to reconstruct the signal exactly. In principle, computing this reconstruction should involve counting non-zeros with L_0. This is a combinatorial problem whose computational complexity makes it impractical. So L_0 can be replaced byL_1. This optimization problem, also known as Basis Pursuit, is significantly more approachable and can be solved with traditional linear programming techniques whose computational complexities are polynomial in N. According to the theory, more than K+1 measurements are required to recover sparse signals via Basis Pursuit. Instead, one typically requires M = cK measurements, where c>1 is an oversampling factor. To recover back X from Y, it is required to estimate the sparsest solution to $Y = \Omega f$, where $\Omega = \Phi\Psi$. Once f is known with the knowledge of Ψ, X can be recovered. The problem of estimating the sparse solution can be posed as

$$\min_{1} \|f\| \text{ subject to } Y = \Omega f \tag{3}$$

By solving for L_0 -norm, the problem gets transformed into a linear programming problem which is quite straight forward.

III. SVD Based Watermarking

An image can be decomposed using SVD to get two orthogonal matrices and one diagonal matrix i.e. $A = U \sum V^T$. Since U and V are orthogonal matrices, manipulations in those matrices are not advisable. The singular values $\sum$ can be utilized for doing manipulations to insert watermark. The important property of singular values is that the modified singular value changes very little after performing attacks. The SVD based watermarking algorithms are composed of an embedding algorithm to embed the watermark(w) in the original image and an extraction algorithm to extract the watermark,where the positive constant α is the scale factor which controls the strength of the watermark to be inserted.

A. *Embedding Algorithm*

It consists of the following steps.

1. $A = \mathbf{U}\Sigma\mathbf{V}^T$
2. $\Sigma_n = \Sigma + \alpha W$
3. $\Sigma_n = U_w \Sigma_w V_w^T$
4. $A_w = U\Sigma_w V^T$

In the First step of the algorithm, the cover image is decomposed in to three matrices U, Σ and V^T. Here W is the encrypted and compressed secret image. In the second step, W is embedding in to the Σ matrix. The resulting matrix is represented by Σ_n. In the third step, Σ_n is again decomposed in to three matrices U_w, Σ_w andtranspose of V_w.In the fourth step, A_w is obtained by combining the U, Σ_w and V^T. A_w is the resulting stegoimage, which hides the encrypted secret data.

B. *Extraction Algorithm*

The extraction algorithm requires U_w , Σ and V_w for extraction.

1. First Step

$$A^*_w = U^* \Sigma^*_w V^{*T}$$

2. Second Step

$$D^* = U_w \Sigma^*_w V_w^T$$

3. Third Step

$$W^* = \frac{1}{\alpha} D^* - \Sigma$$

In the first step of the extraction algorithm the received stegoimage, A^*_w is decomposed in to three matrices U*,$\Sigma^*_w$and V^{*T}. In the second stepD* is obtained by combining U_w, Σ^*_w andV_w^T. In the third step the encrypted secret image, W is obtained from D* and Σ .

IV. Combined Crypto-Steganography

The authors of the paper[16] and [17] discussed the strength of Combined Crypto-Steganography. The proposed system employs the strength of cryptography and steganography to improve the security of the images.

A. *Encryption System*

In the proposed encryption system, the secret image is encrypted using compressive sensing. Encryption of the image is done by performing a linear measurement step. It is achieved by using a measurement matrix. The measurement matrix(Φ) is generated by using a secret key. The resulting encrypted and compressed measurements (Y) are converted in to a matrix format. This is our cipher image. This cipher image is embedding in the cover image using SVD based embedding method. The resulting image is the stego image. Figure.1 shows the proposed combined encryption and embedding stage for the images.

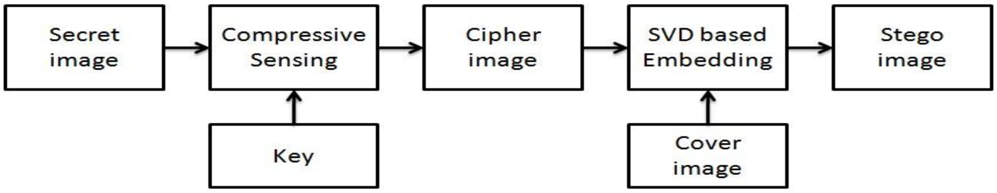


Figure 1: Combined Encryption and Embedding Stage for the Images

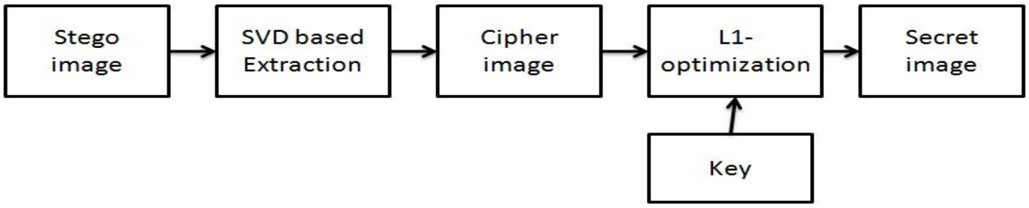


Figure 2: Combined Decryptionand Extracting Stage for Cipher Images

(a) (b)

Figure 3: Input Images for the Proposed System

(a) (b)

Figure 4: Encrypted Secret Image and Stego Image of the Proposed System

(a) (b)

Figure 5: Extracted Image and Decrypted MRI Image

B. Decryption System

In this decryption system, the stego image is extracting using SVD based extraction method. The obtained cipher image is decrypted or reconstructed by using L_1optimization method. Here the same secret key is used to generate the measurement matrix at the reconstruction stage.Figure.2 shows the proposed combined decryption and extraction stage for the encrypted images. So the receiver, who knows the correct key can decrypt the extracted image.

V. Results Obtained for Combined Crypto-Steganography

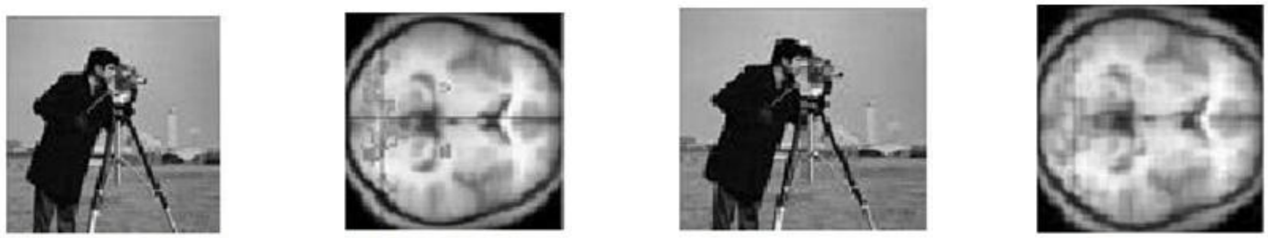
In this system, we take Lena image of size 90×90 as cover message. The cover message is shown in fig. 3(a). We perform SVD on this cover image. We get three matrices such as$U$,Σ and V^T. A MRI image of size $90\times 90$is taken as a secret message. It is shown in the figure 3(b). We are performing compressive sensing on this secret message. First we convert this secret image in to a vector of size8100×1. Then the measurement matrix of size 6400×8100 is generated, using a secret key. The vector is projected on to the measurement matrix. So we get a compressed measurement vector of size6400×1 . These compressed measurements are in an encrypted form. This vector is converted in to a matrix of size 80×80 . The encrypted secret message is shown in the figure 4(a). This matrix is embedded in to the cover image. So this method helps to protect the encrypted and compressed data from the intruders.This encrypted message is embedded in the cover message using SVD based watermark embedding method. Since the secret message is encrypted, it providesmore security to the data hided in the cover message. Figure 4(b) shows the stego message, obtained after secret message is embedded in the cover message.

In the decryption stage, the secret data is extracted using the SVD based water mark extraction algorithm. The extracted encrypted image is shown in figure 5(a). The reconstruction of the encrypted data is done with L_1 optimization.

After the extraction of the encrypted secret data, we perform the compressive sensing based reconstruction. Figure 5(b) shows the decrypted image. The paper [18] discusses the various security analysis of the compressive sensing method. This combined system enhances the security of the data embedded. This method is very useful to encrypt medical and satellite images. The results demonstrate that the proposed system is highly efficient and a robust system.

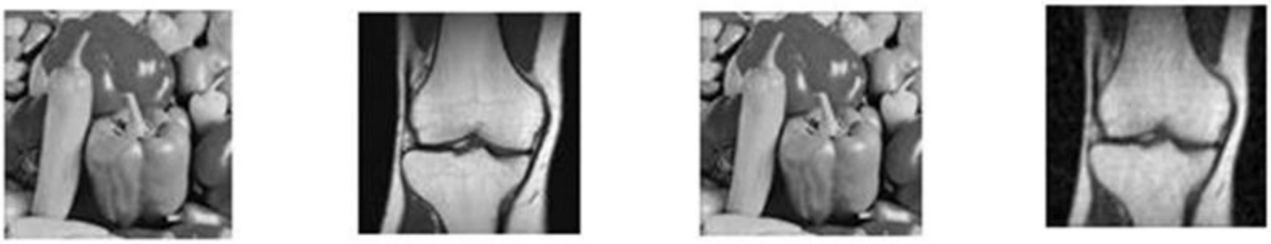
VI. Experiments

Experiments are conducted using different cover images and secret images. Figures 6 to 9 show the results obtained using the proposed encryption scheme using different cover images and secretimages Figure6 shows the result obtained by usingCameraman image as the cover image and a MRI image as secret image. Figure 7 shows the result obtained by using Fruits image as the cover image and a MRI image as secret image. Figure 8 shows the result obtained by using Baboon image as the cover image and a MRI image as secret image. Figure 9 shows the result obtained by using Lady image as the cover image and a MRI image as secret image. Different MRI images are taken as the secret images. In the experiments each original cover image have a size of90×90. Figures 6(a) to 9(a) show the original images, which is taken as the cover image. The secret MRI image has a size of90×90. Figures 6(b) to 9(b) show the secret images. The encrypted image and compressed image is obtained using compressive sensing. The resulting encrypted image is hided in the cover image. The resulting stego images are shown in figures 6(c) to 9(c). Figures 6(d) to 9(d) show the decrypted images using the proposed decryption system.



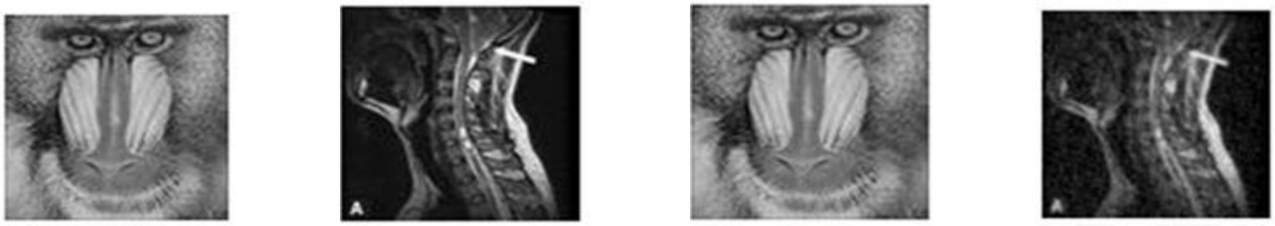
(a) Original Text (b) Secret Text (c) Stego Text (d) Decrypted Text

Figure 6: Results Obtained while using Cameraman Image as Cover Image



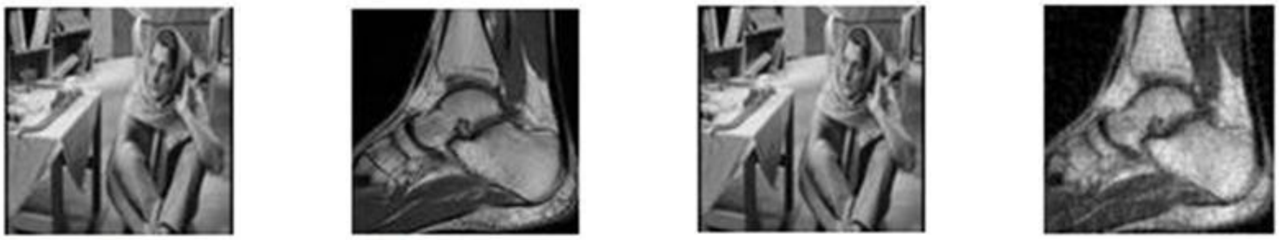
(a) Original Text (b) Secret Text (c) Stego Text (d) Decrypted Text

Figure 7: Results Obtained while using Fruits Image as Cover Image



(a) Original Text (b) Secret Text (c) Stego Text (d) Decrypted Text

Figure 8: Results Obtained while using Baboon Image as Cover Image



(a) Original Text (b) Secret Text (c) Stego Text (d) Decrypted Text

Figure 9: Results Obtained while using Lady Image as Cover Image

VII. Quality of the Proposed Encryption System

The paper [18] discusses the number of measuring techniques to judge the quality of encryption. Peak signal-to-noise ratio can be used to evaluate an encryption scheme. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plain text image and the cipher text image. To compute the PSNR, first calculates the mean-squared error using the equation (4).

$$MSE = \sum_{M,N} \frac{[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (4)$$

In the equation (4), M and N are the number of rows and columns in the input images respectively. The PSNR is obtained by using the equation (5).

$$PSNR = 10 \times \log_{10} \frac{R^2}{MSE} \qquad (5)$$

In the equation (5), R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc. Lower value of PSNR represents better encryption quality. Higher value of PSNR represents superiority of the signal to that of the noise. The table 1 shows the values of PSNR obtained for different cover images and secret images. Thus the proposed encryption system provides better encryption quality comparing with the traditional data hiding scheme [20].Although the decryption capability of proposed system has some limitations, this can be well suited for many other applications other than medical diagnostics. For enhancing the decrypting quality, theright set of random numbers has to be used. However the proposed system proves to be better in maintaining high level of secrecy.

Table 1: PSNR Obtained for Different Cover Images and Secret Images

Cover image	Secret image	PSNR of cover image and stego image	PSNR of secret image and decrypted secret image
Lena	MRI image1	56.397861dB	7.12dB
Cameraman	MRI image 2	51.074098dB	7.43dB
Fruits	MRI image 3	53.717018dB	8.27dB
Baboon	MRI image 4	61.148135dB	8.64dB
Lady	MRI image 5	55.717856dB	7.96dB

VIII. Security Analysis

The paper [19] discusses the various security analysis on the compressive sensing based encryption system. The two possible attacks on compressed sensing based encryption schemes for sparse signals are a brute force attack and attack based on symmetry and sparsity structure [6]. The key length used in the encryption determines the practical feasibility of performing a brute-force attack. Application of at least six keys to encrypt the images in the proposed encryption system increases the difficulty of decryption by this attack. Attack Based on Symmetry and Sparsity Structure is a more informed signal processing attack that exploits the symmetry and sparsity structure inherent in compressed sensing. The complexity of this structured attack is too high to be practical. Statistical analysis and sensitivity analysis were carried out. A. Key Sensitivity Analysis The proposed image encryption procedure should be sensitive with respect to secret key. To prove the robustness of the proposed scheme, sensitivity analysis with respect to key is performed. High key sensitivity is required by secure image cryptosystems, which means the cipher image cannot be decrypted correctly even if there is only a small difference between the encryption and decryption keys. Fig. 10(a) is the original cover image. Fig. 10(b) is the secret image. Fig. 10(c) shows the decrypted secret image with original key. Fig. 10(d) shows the decrypted image with a key, which is close to the original key. From the figure 10, it is clear that even a small change in the encrypted image will cause a drastic change in the decrypted image.

IX. Conclusion and Future Enhancement

A secure encryption scheme by combining the strengths of compressive sensing method and steganography based on SVD based water marking is presented in this paper. By combining, the data encryption can be done by a compressive sensing software and then embed the cipher text in an image or any other media. The combination of these two methods will enhance the security of the data embedded. This method also provides an effective way to compress the data. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The proposed method can be employed on the audio and video data also as a future enhancement.

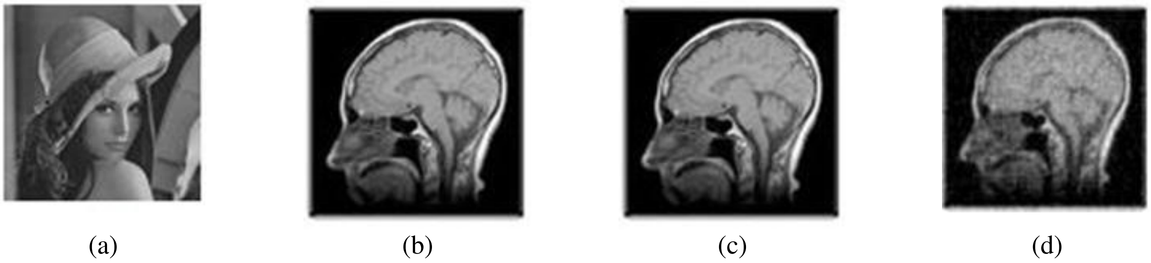


Figure 10: Key Sensitivity Analysis on the Proposed System

References

[1] M.R. Mayiami, BabakSeyfe and H.G. Bafghi, “Perfect Secrecy Using Compressed Sensing”,IEEE Trans, Pp.1-3, 2010.

[2] Y. Rachlin and D. Baron, “The Secrecy of Compressed Sensing Measurements,” Forty-Sixth Annual Allerton Conference, Allerton House, UIUC, Illinois, USA, vol. 52, September 23-26,Pp.813-817,IEEE Trans2008.

[3] R.Huang and K.Sakurai, “A Robust and Compression-combined Digital Image Encryption Method Based on Compressive Sensing”, Seventh

International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pp.105-108, 2011.

[4] A.Orsdemir, H. OktayAltun, G.Sharmaand Mark F. Bocko, "On The Security And Robustness Of Encryption Via Compressed Sensing", IEEE Trans 2008.

[5] Li-Wei Kang, Chun-Shien Lu, and Chao-Yung Hsu, "Compressive Sensing-Based Image Hashing", 16th International Conference on Image Processing (ICIP), Pp.1285-1288, 2009.

[6] Amir M. Abdulghani and Esther Rodriguez-Villegas, "Compressive Sensing: From "Compressing while Sampling" "Compressing and Securing while Sampling", IEEE Conf, Pp.1127-1130, 2010.

[7] A. Anil Kumar and A. Makur, "Lossy Compression of Encrypted Image by Compressive Sensing Technique", IEEE Region 10 Conference, Pp.1-5, TENCON 2009.

[8] Emmanuel .J. Cands and Michael .B. Wakin, "An Introduction To Compressive Sampling", IEEE signal processing magazine [21] , Pp.21-30, March 2008.

[9] Charles J. Colbourn, Daniel Horsley, and Christopher McLean, "Compressive Sensing Matrices and Hash Families", IEEE Transactions on Communications, Volume 59, Issue 7, Pp.1840-1845, 2011.

[10] D. L. Donoho, "Compressed sensing", Inform.Theory IEEE Trans, vol. 52, Pp.1289-1306, July 2006.

[11] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles:Exact signal reconstruction from highly incomplete frequency information" , Inform. Theory IEEE Trans, Volume 52, Pp.489-509, Feb. 2006.

[12] Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data", IEEE on Signal Processing, Volume 51, Pp.2992-3006, Oct 2004.

[13] Candes and M.Wakin, "An introduction to compressive sampling", IEEE Sig. Proc. Mag., Volume 25, Issue. 2, Pp.21-30, Mar.2008.

[14] K. P Soman, K.IRamachandran, N.G Resmi.: "Insight into Wavelets From Theory to Practice", PHILearning Private Ltd, New Delhi,2010.

[15] K. P. Soman and R. Ramanathan, "Digital Signal and Image Processing-The sparse way", ELSEVIER Science and Technology book, 2012.

[16] A.J. Raphael andDr.V. Sundaram, "Cryptography and Steganography–A Survey", Int. J. Comp. Tech. Appl., Volume 2 (3), Pp 626-630.

[17] I.VenkataSaiManoj, "Cryptography and Steganography",International Journal of Computer Applications (0975 – 8887), Volume 1, No.12. , 2012.

[18] Jawad Ahmad and Fawad Ahmed,"Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video& Image Processing and Network Security IJVIPNS-IJENS, Volume 12, No:04, Pp.18-31,August 2012.

[19] Sreedhanya.A.V and Dr. K. P. Soman, "Secrecy OfCryptography With Compressed Sensing", International Conference on Advances in Computing and Communications, Pp.207-210, IEEE 2012.

[20] G.-S. Lin, H. T. Chang, W.-N.Lie, and C.-H. Chuang, "A public-key-based optical image cryptosystem based on data embedding techniques", Optical Engineering, Volume 42, no. 8, Pp.2331-2339, 2003.

Sreedhanya.A.V received B.Tech in Information Technology from the University of Calicut. She had completed M.Tech in Remote Sensing and Wireless Sensor Networks from Amrita School of Engineering, Coimbatore, India. She is currently working as Assistant Professor, Dept of IT, MEA Engineering College, Malappuram, Kerala, India Her research interest includes Compressed Sensing, Cryptography, Image Processing,Remote Sensing, GIS and Wireless Sensor Networks. (*E-mail: sreedhanya1988@gmail.com*)

Dr.K.P. Soman, Professor and Head Computational Engineering and Networking, Amrita School of Engineering, Coimbatore, India.Written books on Sparse Signal and Image Processing, Wavelets, Datamining, Support Vector machines.Currently working in Geometric Algebra, Control theory, Unmanned Aerial vehicles and Wireless sensor network for Aquaponics.(*Email: kp_soman@amrita.edu*)