I.J. Image, Graphics and Signal Processing, **2016, 10, 53-63**
Published Online October 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2016.10.07

Evaluation Compressive Sensing Recovery Algorithms in Crypto Steganography System

F. Kafash Ranjbar
Electrical and Electronic Engineering Department, Islamic Azad University, South Tehran Branch, Tehran, Iran.
Email: St_F_KafashRanjbar@azad.ac.ir

S. Ghofrani*
Electrical and Electronic Engineering Department, Islamic Azad University, South Tehran Branch, Tehran, Iran.
Email: S_Ghofrani@azad.ac.ir

***Abstract*—**The main contribution of this paper is using compressive sensing (CS) theory for crypto steganography system to increase both the security and the capacity and preserve the cover image imperceptibility. For CS implementation, the discrete Cosine transform (DCT) as sparse domain and random sensing matrix as measurement domain are used. We consider 7 MRI images as the secret and 7 gray scale test images as cover. In addition, three sampling rates for CS are used. The performance of seven CS recovery algorithms in terms of image imperceptibility, achieved peak signal to noise ratio (PSNR), and the computation time are compared with other references. We showed that the proposed crypto steganography system based on CS works properly even though the secret image size is greater than the cover image.

***Index Terms*—**Decryption, encryption, image steganography, singular value decomposition (SVD), compressive sensing (CS).

I. Introduction

Recent years, data hiding including steganography and watermarking is important due to internet and telecommunication rapid development. There are three main attributes to be observed in a data hiding system known as capacity, imperceptibility, and robustness. The main issue for steganography is capacity where as the main concern for watermarking is robustness [1].

In general, the task of a steganography system is embedding data into a cover image and transferring to the destination without being detected not only by human visual system (HVS) but also by powerful machine vision techniques or steganalysis algorithms. The steganography are performed [2] either in spatial domain [3] or in transformed domain [4], [5].

Cryptography merely obscures the integrity of information so that it does not make sense to anyone except the administrator [6]. A cryptographic algorithm can be classified based on the number of keys used for encryption and decryption [7]. Accordingly, there are two groups of cryptography systems. The first group named symmetric key system uses single key for both sender and the receiver. The second group named public key system or asymmetric key system uses two keys, a public key which everyone knows and a private key that only the recipient knows. Although, the asymmetric key system enables secure communication via insecure channels, the symmetric key system is faster. RSA is an example of asymmetric key encryption system [6], [8].

While steganography and cryptography are both used to ensure data confidentiality, the cryptography focuses on keeping the contents of a message secret and the steganography focuses on keeping the existence of a message secret [6]. So, high security is achieved by using both steganography and cryptography as well [9], i.e. the encrypted message is hiding by steganography [6].

The traditional approach of reconstructing signals or images from measured data follows the well known Shannon sampling theorem [10] which states that the sampling rate must be twice the highest frequency. Recently, the theory of compressive sensing (CS) or sparse representation showed that a signal can be precisely reconstructed from only a small set of measurements if the signal be sparse. Sparsity has a rich history of applications in signal processing problems including de–noising, de–convolution, restoration and in painting [11]- [13]. It has been observed that sparse representation of signals provide very high compression ratios. Hence, it makes sense to exploit sparsity of signals for hiding secret message in steganography.

This ability of sparse representation was considered for encrypting image folding [13], and for image steganography [1]. In [14], it was shown that the CS based encryption does not achieve Shannon's definition of perfect secrecy, but can provide a computational guarantee of secrecy. In [15], it was demonstrated that the CS based encryption under some circumstances achieves perfect secrecy.

In this paper, we use the compression and encryption data by CS theory. In CS, compression and encryption is achieved by a single linear measurement step. This step is performed by using a measurement matrix, the resultant compressed measurements are encrypted using asymmetric encryption algorithms that generated by RSA algorithm, next level of security to the compressed and encrypted data is provided with the help of steganography. This encrypted and compressed data is embedded in the cover or host image by using the singular value decomposition (SVD) algorithm. The resultant stego image is transmitted through the network. In receiver side, stego image is received and the CS recovery and decryption algorithms are used to get the secret image. In this paper, two groups of CS recovery algorithms (greedy and convex optimization) in terms of PSNR and time consuming are evaluated. The proposed system satisfies the explained conditions in [15] and achieves better results rather than the recent survey in [16]. Furthermore, a secret image greater than a cover image can be hidden and recovered as well.

This paper is organized as follows. Section 2 provides a background of this work including CS and cryptography by RSA and SVD based watermarking. Section 3 explains the proposed method that is crypto steganography based on CS theory. Section 4 gives the experimental results and compares the proposed method with six research papers [16]- [21]. Finally, Section 5 concludes the paper.

II. Reviewing CS, RSA, SVD

In general, CS theory requires that the sensed signal to be sparse in a given orthogonal basis and the sensing vectors to be incoherent with this basis. Due to the vast interest in this topic, there exist several review articles on the basics of CS [22]- [26].

A. Compressive Sensing (CS) Theory

CS relies on two principles; sparsity and incoherency. A signal is sparse if it only has few nonzero elements, or it is approximately sparse if it has few large elements and other elements are nearly zero. CS theory exploits the fact that many natural signals are sparse and so compressible when they are expressed in the proper basis. For example a Dirac or a Spike is sparse in time domain where as a sinusoid is sparse in frequency domain. The coherence property is defined between the measurement or sensing matrix, $\mathbf{\Phi}$, with size $m\times n$, and the basis or sparse basis matrix, $\mathbf{\Psi}$ with size $n\times n$,

$$\mu(\mathbf{\Phi},\boldsymbol{\psi})=\sqrt{n}\max_{1<z,j<n}|<\mathbf{\Phi}_z,\boldsymbol{\psi}_j>| \tag{1}$$

where $\mathbf{\Phi}_z$ is the *z*–th row of $\mathbf{\Phi}$ and $\boldsymbol{\psi}_j$ refers to the *j*–th column of $\boldsymbol{\psi}$. According to CS theory, the matrices $\mathbf{\Phi}$ and $\boldsymbol{\psi}$ should have maximum incoherency. It was shown that random matrices are largely incoherent with any fixed basis [25]. In this paper, the basis matrix $\boldsymbol{\psi}$ is determined in DCT domain and the measurement matrix $\mathbf{\Phi}$ is considered a random matrix with normally distributed pseudorandom numbers. Based on the CS theory, any observed vector **y** is written as:

$$\mathbf{y}_{m\times1}=\mathbf{\Phi}_{m\times n}\mathbf{x}_{n\times1} \tag{2}$$

where $\mathbf{x}$ is the true signal that can be written in some basis (like Fourier, wavelet, and DCT) as:

$$\mathbf{x}_{n\times1}=\boldsymbol{\psi}_{n\times n}\mathbf{s}_{n\times1} \tag{3}$$

where $\mathbf{s}$ has only k non–zero entries and so called k–sparse. According to (2) and (3), we have,

$$\mathbf{y}_{m\times1}=\mathbf{\Phi}_{m\times n}\boldsymbol{\psi}_{n\times n}\mathbf{s}_{n\times1}=\mathbf{H}_{m\times n}\mathbf{s}_{n\times1} \tag{4}$$

where $\mathbf{H}$ named the dictionary. The CS theory states that such a sparse signal $\mathbf{s}$ can be reconstructed by taking $\mathrm{m} \geq \mathcal{O}\left(\mathrm{k}\log{}^{\mathrm{n}}/_{\mathrm{k}}\right)$ linear, non–adaptive measurements whenever a random sensing matrix $\mathbf{\Phi}$ is used. Furthermore, $\mathbf{\Phi}$ and $\boldsymbol{\psi}$ or $\mathbf{H}$ must satisfy the restricted isometric property (RIP) [23]. To support this theory, the sampling rate below Nyquist is considered. Suppose that $m\geq 2k$ and $\mathbf{\Phi}$ has a uniform distribution and satisfies RIP. If there is not any null message in the set of source messages, perfect secrecy will be achieved via CS [15].

For underdetermined problem, with $m<<n$, Eq. (4) does not have unique solution. In this case, the sparse recovery algorithms reconstruct the sparsest $\mathbf{s}$ by solving the following optimization problem:

$$\text{minimize } ||\hat{\mathbf{s}}||_1 \quad \text{subject to } \quad \mathbf{y}=\mathbf{H}\hat{\mathbf{s}} \tag{5}$$

where ℓ_1 norm, defined as $||\mathbf{x}||_1=\sum_n|\mathbf{x}[n]|$. Often the observed vector includes additive noise, so it is modeled as:

$$\mathbf{y}_{m\times1}=\mathbf{H}_{m\times n}\mathbf{s}_{n\times1}+\mathbf{e}_{m\times1} \tag{6}$$

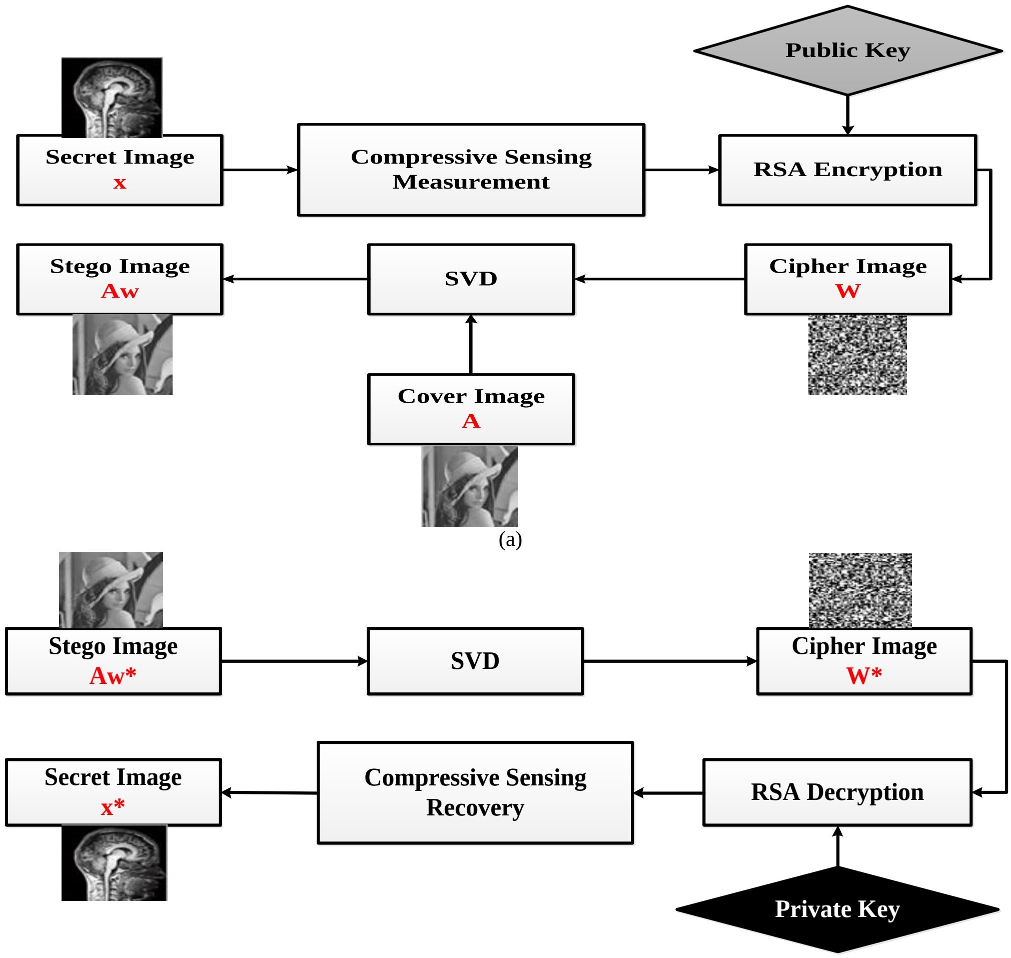
where $\mathbf{e}$ is a stochastic or deterministic error term with bounded energy $||\mathbf{e}||_2<\varepsilon$ and ℓ_2 norm defined as $||\mathbf{x}||_2=\sum_n|\mathbf{x}[n]|^2$. Then, the sparsest $\mathbf{s}$ is obtained by solving the following optimization problem,

$$\text{minimize } ||\hat{\mathbf{s}}||_1 \quad \text{subject to } \quad ||\mathbf{y}-\mathbf{H}\hat{\mathbf{s}}||_2<\varepsilon \tag{7}$$

So far, different methods named recovery algorithms have been developed for solving the underdetermined or sparse approximation problems which may broadly be grouped into five different categories [27]. The first group includes greedy algorithms such as the matching pursuit, orthogonal matching pursuit (OMP) [28], compressive sampling orthogonal matching pursuit (CoSaMP) [29] and accelerated iterative hard threshold (AIHT) [30]. The second category of approaches are based on convex optimization like the basis pursuit (BP), focal underdetermined system solver (FOCUSS), L1–Magic toolbox [31] and fixed point continuation (FPC) [32]. The third group is based on some statistical parameters such as the maximum a posteriori (MAP) or minimum mean square error (MMSE). Apart from these, the fourth group is based on non–convex optimization and the fifth group is Brute Force [33] which are not popular.

In this paper we survey the first and the second categories i.e. greedy algorithms and convex optimization.

The greedy algorithms include OMP, CoSaMP and AIHT. In convex optimization we use L1–Magic toolbox that consist of minimum energy (ME) that is initial guess from solution for some of algorithms which require initial value, L1_eq and TV1 that solve equality constrained total variation (TV) minimization, another algorithm that survey in convex optimization group is FPC.



(a)

(b)

Fig.1. The block diagram of the proposed method for (a) embedding and (b) extracting.

B. Cryptography by RSA Algorithm

The RSA algorithm was proposed in 1977 [6], [8]. The procedures of generating RSA either for public key or private key are written in following [34],

1. Choose two prime numbers, named p and q, then obtain N= pq.
2. Choose a number E, where it is relatively prime to Z= (p-1)(q-1). It means that the greatest common divisor (gcd) of E and Z is 1, i.e. gcd (E, Z)=1 and 1 <E<Z . The pair (N, E) is the public key.
3. Obtain an integer d as a private key where Ed=1 (mod Z) and mod refers to the remainder of a division.

A message “M” with the public key (N, E) is encrypted and the cipher text “C” is generated as,

$$C = M^{E} \ \mathbf{mod} \ N \tag{8}$$

Then at the receiver, the cipher text $'C'$ is decrypted by using the known “private key”,

$$M = C^{\mathbf{d}} \ \mathbf{mod} \ N \tag{9}$$

The above explained procedures are performed for all pixels of an image. Therefore, the image is encrypted by RSA algorithm.

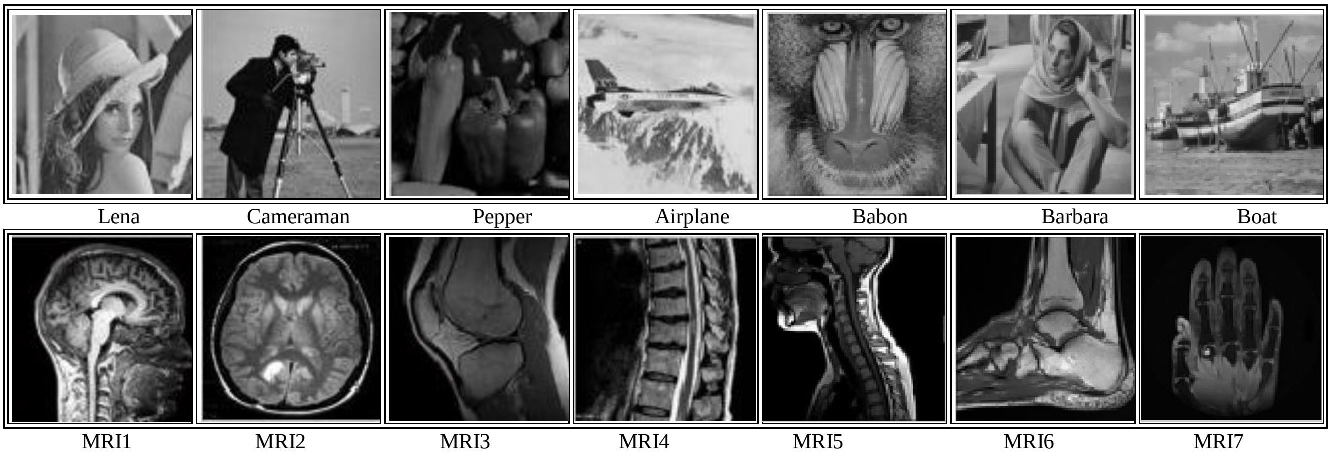
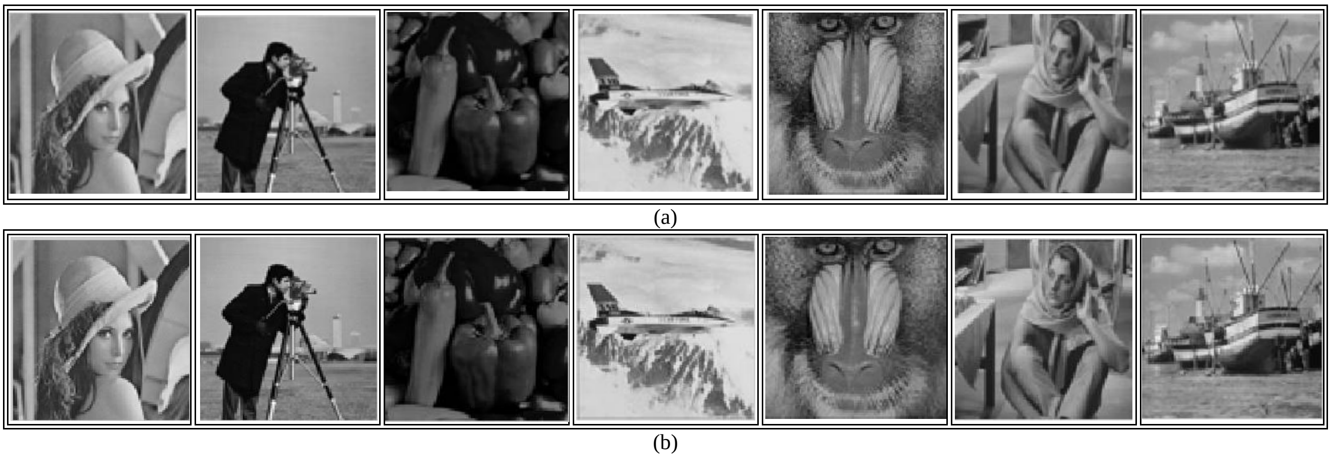


Fig.2. Shown cover images (first row) and the corresponding secret images (second row).


(a)

(b)

Fig.3. Stego images are shown for the sampling rate 34% . (a) the secret image size is the same as the cover image, (b) the secret image size is greater than the cover image.

C. Steganography by SVD Based Watermarking

SVD has been used for different applications such as compression [35], hiding [36], [37], and watermarking [38]. Given a digital image matrix as $\mathbf{A}$ with size $\sqrt{n} \times \sqrt{n}$, the SVD of real matrix $\mathbf{A}$ is:

$$\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}V^T = \begin{pmatrix} u_{11} & \cdots & u_{1\sqrt{n}} \\ \vdots & \ddots & \vdots \\ u_{\sqrt{n}1} & \cdots & u_{\sqrt{n}\sqrt{n}} \end{pmatrix} \begin{pmatrix} \delta_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \delta_{\sqrt{n}\sqrt{n}} \end{pmatrix} \begin{pmatrix} v_{11} & \cdots & v_{1\sqrt{n}} \\ \vdots & \ddots & \vdots \\ v_{\sqrt{n}1} & \cdots & v_{\sqrt{n}\sqrt{n}} \end{pmatrix} \tag{10}$$

where $\mathbf{U}$ and $\mathbf{V}$ are orthogonal matrix including the eigen vectors, $\mathbf{(.)^T}$ refers to the transpose operation and $\boldsymbol{\Sigma}$ is the diagonal matrix containing the singular value entries or eigen values in which

$$\delta_{11} \ge \delta_{22} \ge \ldots \ge \delta_{rr} = \ldots = \delta_{\sqrt{n}\sqrt{n}} \ge 0 \tag{11}$$

In general, steganography based on using SVD includes the embedding and the extracting algorithms,

- **Embedding**

1. Decompose the cover image, $\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}V^T$.
2. Embed the encrypted and compressed secret image into the diagonal matrix, $\boldsymbol{\Sigma}_{\sqrt{n}} = \boldsymbol{\Sigma} + \alpha\,\mathbf{W}$. Where, α is the scale parameter with positive value that controls the strength of the hidden message. It means that we get the convenient stego image quality for the small value of α .
3. Decompose matrix, $\boldsymbol{\Sigma}_{\sqrt{n}} = \mathbf{U_w}\boldsymbol{\Sigma}_\mathbf{w}\mathbf{V_w^T}$.
4. Obtain the stego image, $\mathbf{A_w} = \mathbf{U}\boldsymbol{\Sigma}_\mathbf{w}\mathbf{V^T}$.

- **Extracting**

The extraction algorithm requires $\mathbf{U_w}$, $\mathbf{V_w}$, $\boldsymbol{\Sigma}$ and α .

1. Decompose the received stego image, $\mathbf{A_w^*} = \mathbf{U^*}\boldsymbol{\Sigma}_\mathbf{w}^*\mathbf{V^{*T}}$.
2. Obtain matrix, $\mathbf{D^*} = \mathbf{U_w}\boldsymbol{\Sigma}_\mathbf{w}^*\mathbf{V_w^T}$.
3. Approximate the encrypted and compressed secret image, $\mathbf{W^*} = \frac{\mathbf{1}}{\alpha}[\mathbf{D^*} - \boldsymbol{\Sigma}]$.

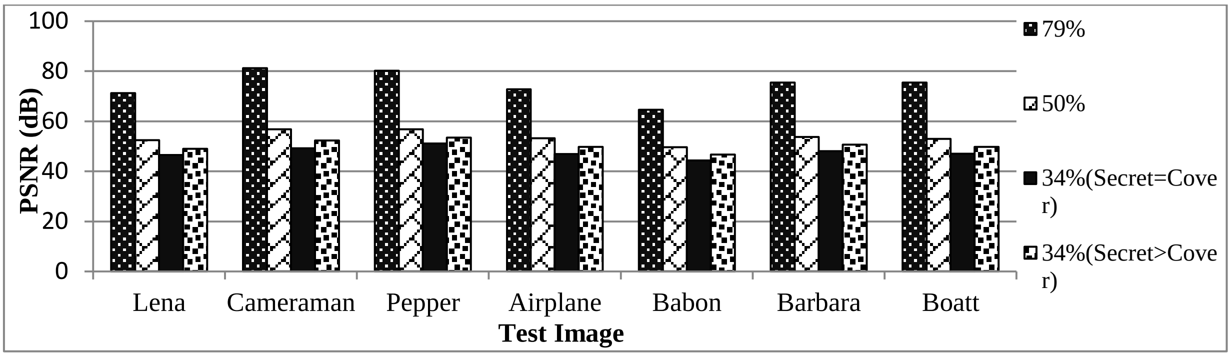
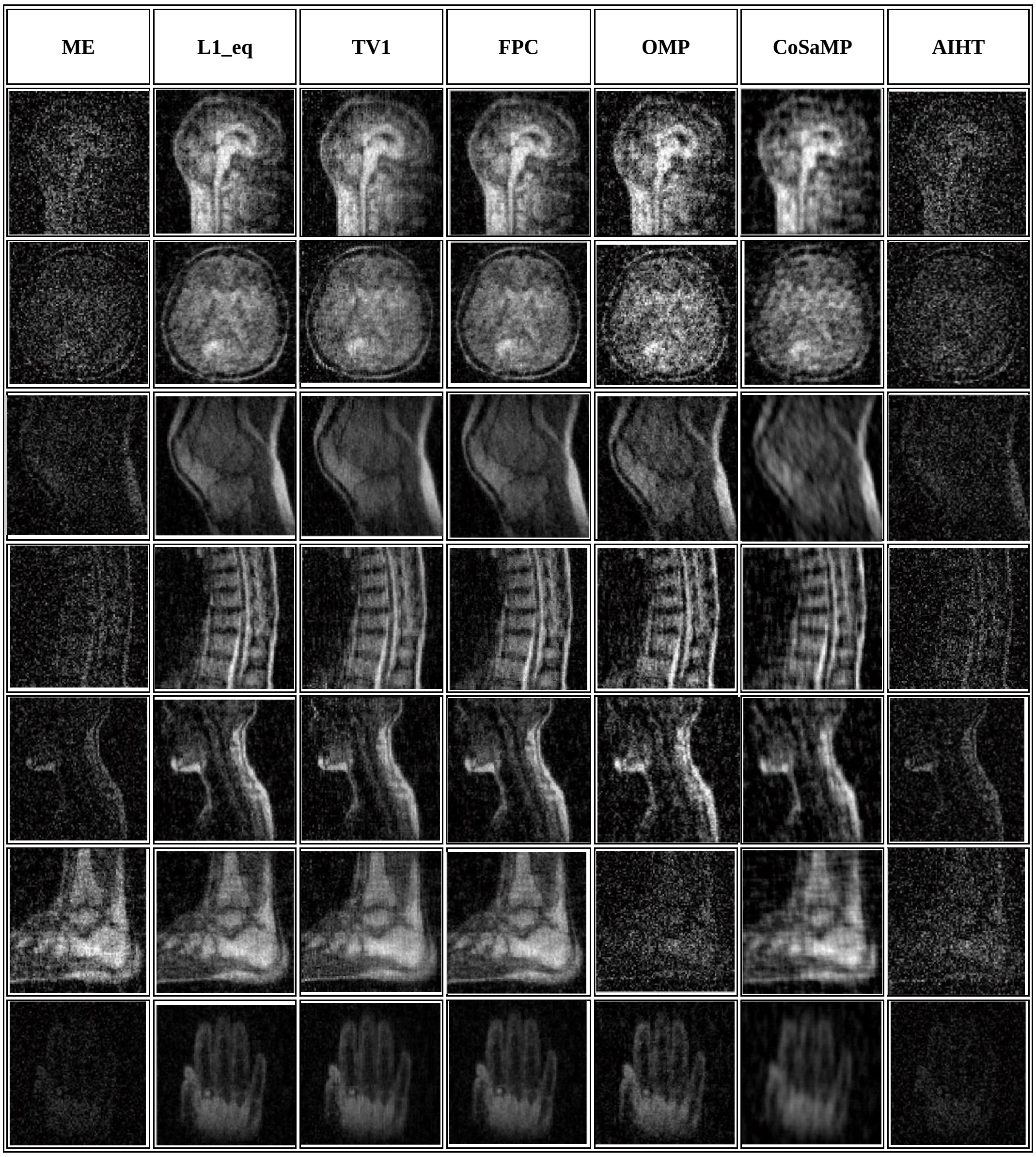
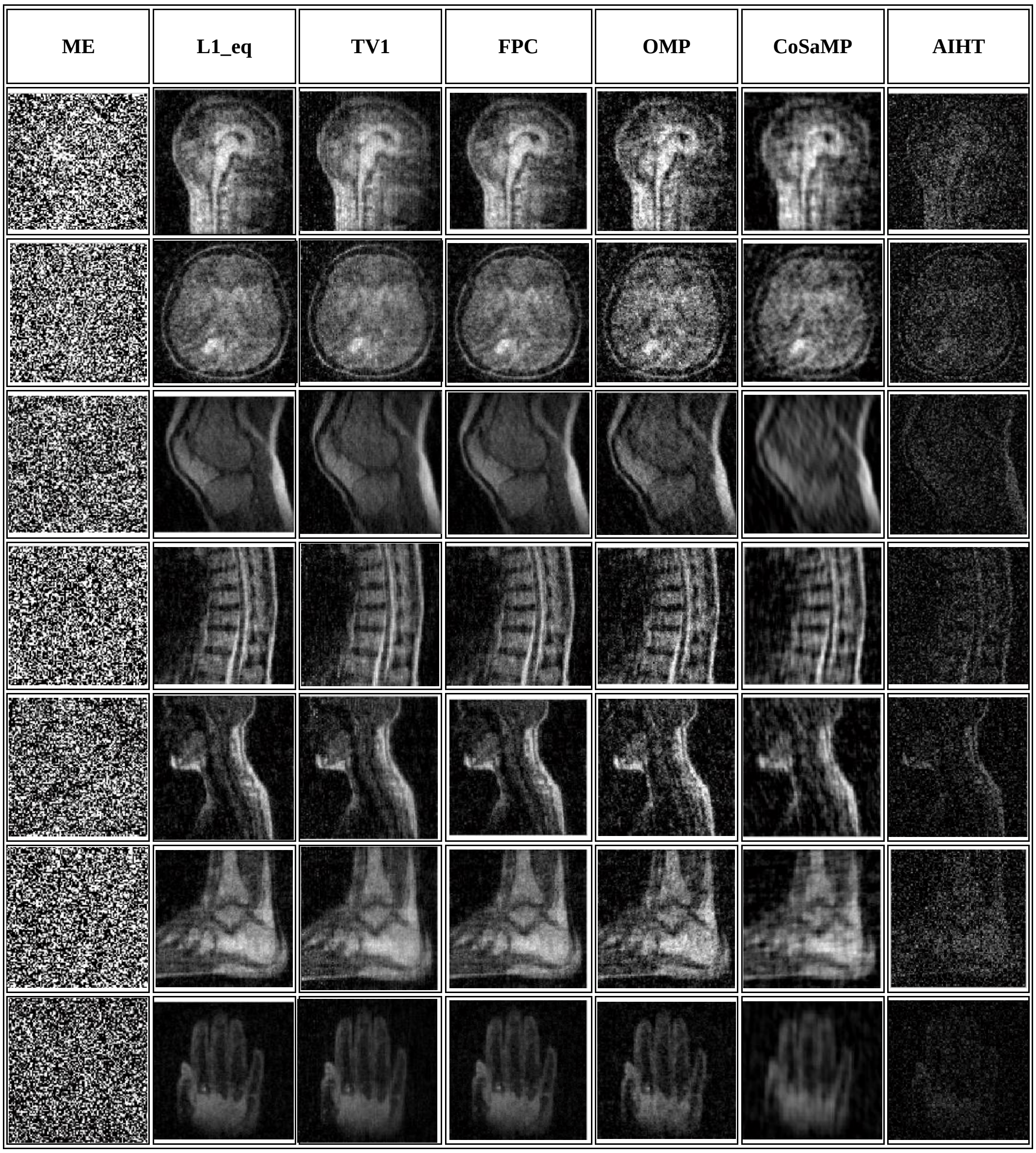


Fig.4. Obtained the PSNRs of 7 stego images for different sampling rates.



(a)



(b)

Fig.5. Shown the extracted hidden images by using 7 different CS recovery algorithms (ME, L1_eq, TV1, FPC, OMP, CoSaMP, AIHT) for sampling rates 34%, (a) secret and cover image are the same size, (b) secret image size is greater than cover image.

III. The Proposed Method

The block diagram of our proposed method is shown in Fig. 1. As seen in Fig. 1-a, using the CS measurement down size the secret image, $'\mathbf{x}'$. Therefore, in addition to more security, the system capacity is also increased. These are the main advantages of the proposed method using CS. The observed vector named $'\mathbf{y}'$ is encrypted by RSA algorithm and the cipher image named $'\mathbf{W}'$ is obtained. The cover image is decomposed by using the SVD and the cipher image is embedded. In this paper, according to experiments, the value of $\alpha = 10^{-7}$. The result image is stego named $\mathbf{A_w}$

In the receiving stage, seen Fig. 1-b, at first the stego image is decomposed by SVD, the obtained cipher image is decrypted by RSA algorithm and then the secret image is recovered by ℓ_1 norm optimization algorithms. In this paper, the private key is used to generate the measurement matrix at the reconstruction stage. So the receiver that knows the correct key, can decrypt the extracted image.

According to [39], any information hiding technique must satisfy the following constraints.

- The perceived quality of the cover message should not be degraded due to embed the stego.
- The detection of the presence of a hidden message and subsequent determination of the same must require the knowledge of some secret “key”.

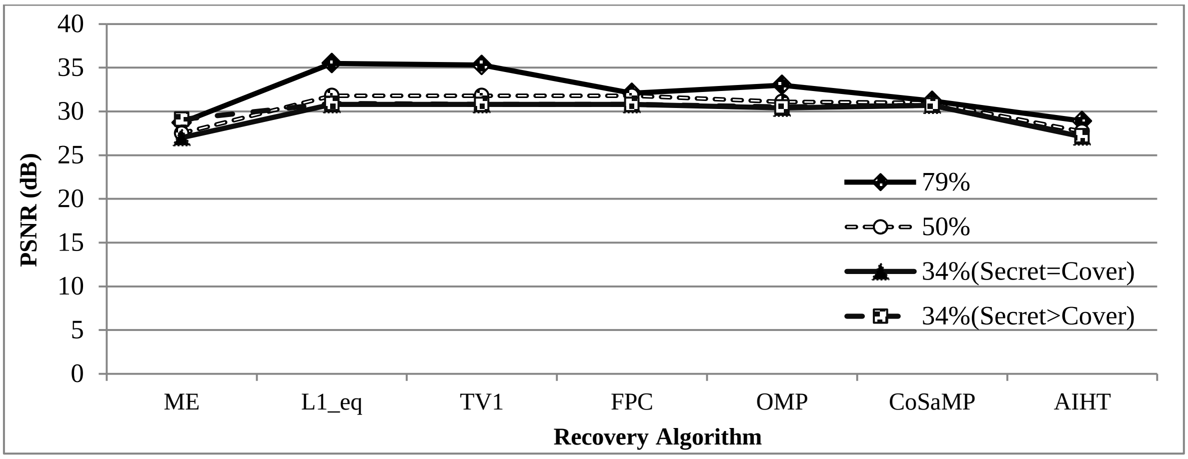


Fig.6. Comparing the performance of 7 CS recovery algorithms based on average PSNRs.

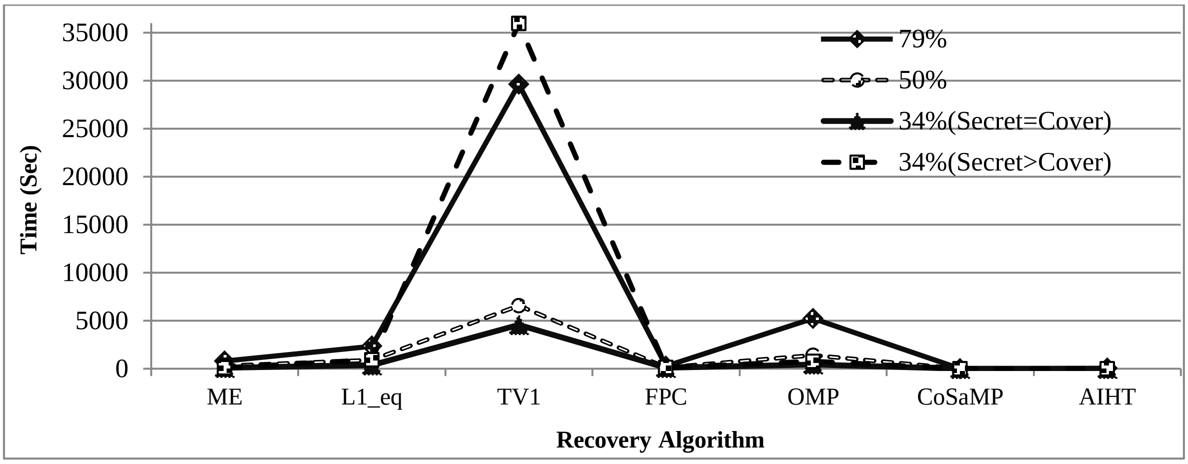


Fig.7. Comparing the performance of 7 CS recovery algorithms based on average time consuming.

- If multiple messages are hidden within the same cover then they should not interfere.
- The hidden message should be robust to the most attacks that do not degrade the perceived quality of the cover message.

Generally, using cryptography and steganography together improve the security of embedded data. This combined chemistry will satisfy constraints in [15] and the requirements such as capacity, security and robustness for secure data transmission over an open channel [6], [8], [34], [40]. In this paper, we show that using CS achieves the appropriate performance, more security and capacity. Furthermore, the secret image size can be even greater than the cover image because of using CS. Accordingly, we get more capacity rather than other crypto steganography systems [16]- [21].

IV. Experimental Results

In this paper, as shown in Fig. 2, we choose 7 test images and 7 MRI images as cover and secret images with the same size, i.e. 90×90 pixels. Then in order to show the CS capability of increasing the steganography capacity, the secret image size is considered 101×101 pixels. The method is implemented by using MATLAB R2012b on a PC with CPU 2.20 GHZ 2Duo and RAM 4GB. At first, the secret images with size 90×90 and 101×101 pixels ($\mathbf{x}_{\sqrt{n}\times\sqrt{n}}$) are vectorized into 8100×1, and 10201×1 ($\mathbf{x}_{n\times1}$), then the observed vector ($\mathbf{y}_{m\times1}$) is obtained based on $\mathbf{y}_{m\times1} = \mathbf{\Phi}_{m\times n}\,\mathbf{x}_{n\times1}$. In order to have the different sampling rate, three random entries sensing matrix $\mathbf{\Phi}$ with size 6400×8100, 4096×8100, and 2809×8100 are generated (the cover and secret are the same size) where the sampling rate are defined as $\frac{m}{n}\times100 \cong 79.5$, 50, and 34%. Furthermore, in order to show that the CS increases the steganography capacity and preserves the performance, a sensing matrix $\mathbf{\Phi}$ with size 3364×10201 is also generated (the secret image size is greater than the cover) where the sampling rate is $\frac{m}{n}\times100 \cong 34\%$. According to CPU and RAM hardware limitation, in this case, we couldn't have any implementation for sampling rates 50% and 79%. In following the observed vector $\mathbf{y}_{m\times1}$ is converted into a matrix with size $\sqrt{m}\times\sqrt{m}$ pixels and the matrix is encrypted by RSA algorithm. Then, the cipher image named $\mathbf{W}$ with size $\sqrt{m}\times\sqrt{m}$ pixels is generated.

Table 1. Details of references for comparison with the proposed system.

References	Compressed Sensing	Steganography algorithm	Cryptography algorithm
[16]	Yes	Adaptive steganography in transform domain	Symmetric key
[17]	No	Transform domain	Symmetric key
[18]	No	Transform domain	Asymmetric key by RSA
[19]	No	LSB and adaptive steganography in spatial domain	-
[20]	No	LSB and transform domain	Symmetric key
[21]	No	Transform domain and pixel value difference	-
The proposed method	Yes	Adaptive steganography in transform domain	Asymmetric key by RSA

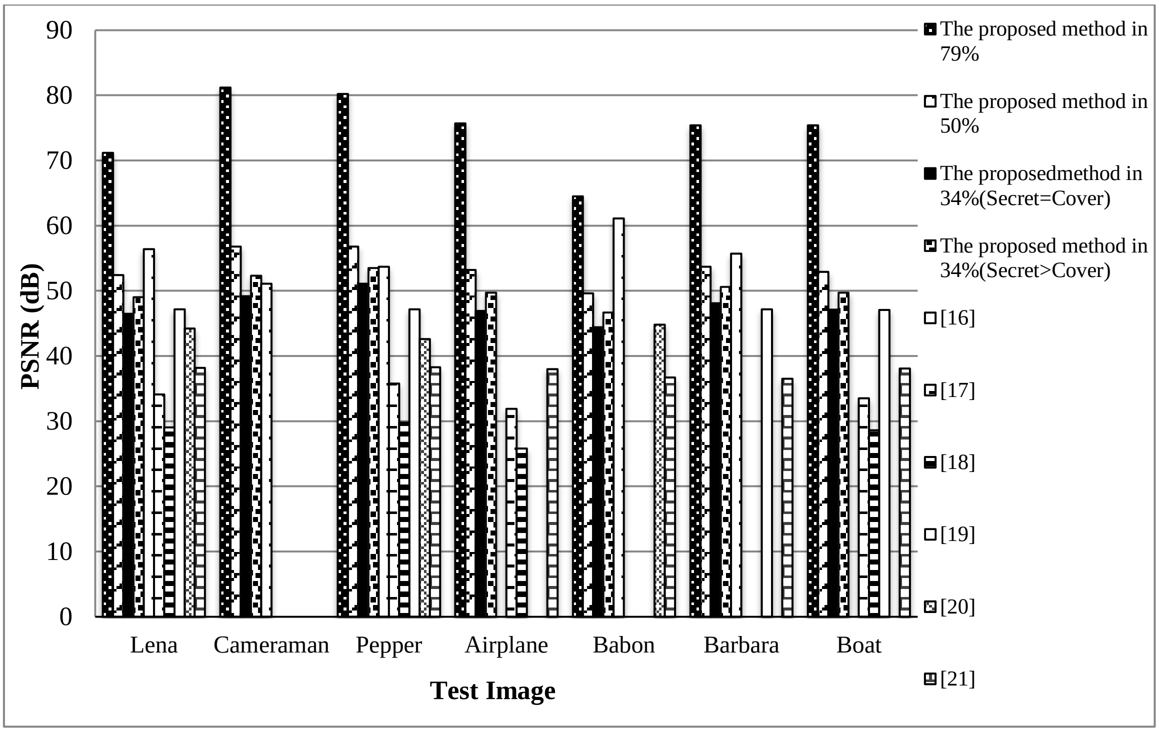


Fig.8. Comparison the proposed method with other references based on PSNR.

At the second step, the cover image with size 90×90 is decomposed by SVD and the $\sqrt{m}$ largest singular values in matrix $\mathbf{\Sigma}$ and the corresponding eigen vectors are obtained. The cipher image is embedded into high frequency of the cover image and the stego image is generated. For large value of *m*, which means selecting more number of the largest SVDs, and small value of α (in this paper $\alpha = 10^{-7}$), the quality of stego image and the capacity would be appropriated.

As we mentioned, in this paper, the embedding rates are 79, 50, and 34% when the secret and the cover images size are the same (90×90 pixels), in this case the embedding and the extracting bytes are 51200, 32768, and 22472 in order, and the embedding rate is 34% when the secret image (101×101 pixels) is greater than the cover image (90×90 pixels), in this case the embedding and the extracting bytes are 26912. Fig. 3, shows the stego images for embedding rate 34% where the secret and the cover images size are the same, Fig. 3-a, and the secret image size is greater than the cover, Fig. 3-b.

This method helps to protect the encrypted and compressed data from the intruders, since the secret message is encrypted, it provides more security to the data hidden in the cover message. According to subjective criteria (human vision), there is no difference between cover image and stego image in Fig. 3. However, the invisibility of the hidden message or the

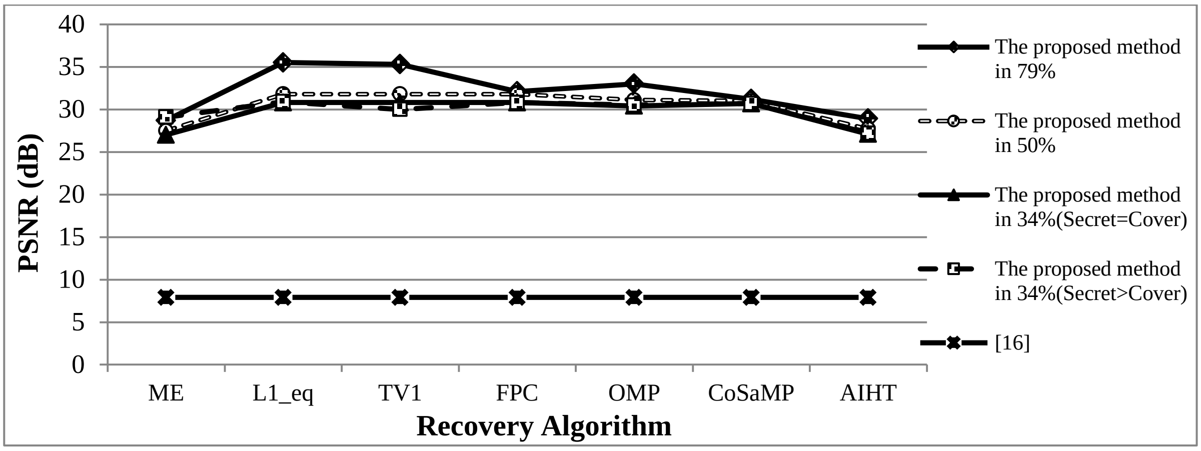


Fig.9. Comparing the performance of 7 recovery algorithms with [16] in terms of PSNR.

quality of stego image is measured in terms of PSNR [41], [42],

$$PSNR = 10\log\frac{R^2}{MSE} \qquad (12)$$

where R for an 8–bit unsigned integer data type is 255, and MSE, refers to mean square error, is used to quantify the difference between the cover image **A** and the stego image $\mathbf{A_w}$,

$$MSE = \sum_{\sqrt{n}\sqrt{n}} \frac{[\mathbf{A}(\sqrt{n},\sqrt{n}) - \mathbf{A_w}(\sqrt{n},\sqrt{n})]^2}{\sqrt{n}\times\sqrt{n}} \qquad (13)$$

where $\sqrt{n}\times\sqrt{n}$ is the image size. PSNR values below 30 dB indicates a fairly low quality, and the PSNR of high quality stego image is greater than 40 dB. Fig.4, shows the achieved PSNR of the proposed method under different situations. The average PSNR for all cases are above 45 dB. Specifically, where the secret and the cover image has the same size, the average PSNRs for 79, 50, and 34% sampling rate are 74.4, 53.6, and 47.6 dB where the secret image is 101×101 pixels and the cover image is 90×90 pixels, and the average PSNR for 34% sampling rate is 50.2 dB. Obviously, in this paper, under different circumstances and for all 7 test images as cover and 7 MRI images as secret images, the achieved PSNR demonstrate the high quality and capacity.

For receiving stage, we follow these steps, the cipher image with size $\sqrt{m}\times\sqrt{m}$ is extracted by using the SVD based watermark extraction algorithm for sampling rates 79, 50, and 34%. In the second step, cipher images are decrypted by using RSA algorithm and a vector with size $m\times1$ is obtained. Finally in the third step, the secret image is recovered according to the different CS reconstruction algorithms. In this paper, the performance of two groups of CS reconstruction algorithms, greedy and convex optimization, are compared in terms of extracted secret image vision quality (see Fig. 5), average PSNR (see Fig. 6), and average time consuming (see Fig. 7).

According to Fig. 5, the ME and AIHT are not recommended. As also seen in Fig. 6, these two algorithms get average PSNR below 30 dB. Although the achieved PSNR by CoSaMP is sufficient, Fig. 5 shows that the extracted secret image is some how blur. The performance of L1_eq, TV1, FPC, and OMP are close according to Figs. 5, 6. So, having a look at Fig. 7, the recovery algorithms are compared in terms of average time consuming.

Accordingly, L1_eq and FPC are candidate as the best recovery algorithms. Furthermore, FPC outperforms whenever there is noise. So, in this paper, FPC is known as an efficient and practical CS reconstruction algorithm. The performance of all algorithms for embedding rate 79% is appropriate in comparison with the embedding rates 50, and 34%. However, a large number of samples increase significantly the recovery processing time as well. At the end, for the sampling rate 34% when the secret image size is greater than the cover image, the CS power for increasing the steganography capacity is seen.

In following, the performance of the proposed method based on CS is compared with other references [16]- [21]. For this purpose, Table. 1, introduces the main characteristics of each algorithm, and Figs. 8, 9 show the achieved PSNRs for different cover images and recovery algorithms. As seen in Fig. 8, the proposed method for embedding rate 79% achieved the best result in comparison with all of mentioned references [16]- [21]. Fig. 9 shows the average PSNRs of seven recovery algorithms for different embedding rates [16] which has close idea to the proposed method, with embedding rate equal 79% . The average achieved PSNR for [16] is 7.9 dB, the recovery algorithm and the time consuming were not reported. The used cover images in [16] were Lena, Cameraman, Pepper, Babon, and Barbara, and the MRI secret images shown in Fig. 2 (second row for this corresponding cover images) were used. As seen in Fig. 9, the proposed steganography method based on CS under different circumstances and for all seven recovery algorithm is appropriate than [16].

V. Conclusion

In this paper, a crypto steganography system based on CS theory was proposed. This method improves the security and increases the capacity easily. Data security is provided by CS and RSA algorithms. The compressed and encrypted data are hidden in cover image by using SVD based watermark embedding method. As sending the encrypted message directly through the medium increases the attention of the intruders, using the compressed and encrypted data in steganography system definitely increase the system security. Furthermore, we showed that using CS not only causes more security but also increases the steganography capacity. It means the system performance via objective and subjective criteria is appropriate even the secret image size is greater than the cover image size.

References

[1] A. Ahani and Sh. Ghaemmaghami, “Image Steganography based on Sparse Decomposition in Wavelet Space,” IEEE International Conference on Information Theory and Information Security (ICITIS), pp. 632–637, 2010.

[2] A. D. Ker, “A Capacity Result for Batch Steganography,” Signal Processing Letters, vol. 14, no. 8, pp. 525–528, 2007.

[3] C. K. Chan and L. M. Cheng, “Hiding Data in Images by Simple LSB Substitution,” Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.

[4] Z. Liang, “Wavelet Domain Steganography for JPEG2000,” IEEE International Conference on Communications, Circuits and Systems Proceedings, vol. 1, pp. 40–43, 2006.

[5] R. Safy, H. Zayed, and A. Dessouki, “An Adaptive Steganographic Technique Based on Integer Wavelet Transform,” IEEE International Conference on Networking and Media Convergence, pp. 111–117, 2009.

[6] A. J. Raphael and V. Sundaram, “Cryptography and Steganography–A Survey,” International Journal of Computer Technology Application, vol. 2, no. 3, pp. 626–630, 2010.

[7] J. Varghese, “Image Encryption and Compression using Embedding Technique,” Master thesis, Department of Computer Science, Christ University Bangalore, 2010.

[8] P. Marwaha, “Visual Cryptographic Steganography in Images,” Second International conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-6, 2010.

[9] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, “A Novel Secure Communication Protocol Combining Steganography and Cryptography,” Advanced in Control Engineering and Information Science, vol. 15, pp. 2767–2772, 2011.

[10] M. Unser, “Sampling—50 Years after Shannon” Proceedings of the IEEE, vol. 88, no. 4, pp. 569–587, 2000.

[11] E. Candes, J. Romberg, and T. Tao, “Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information,” IEEE Transaction of Information. Theory, vol. 52, no. 2, pp. 489–509, 2006.

[12] D. L. Donoho, “Compressed Sensing,” IEEE Transaction of Information Theory, vol. 52, no. 4, pp. 1289–1306, 2006.

[13] J. Bowley, and L. Rebollo-Neira, “Sparsity and Something else: an Approach to Encrypted Image Folding,” IEEE Signal Processing Letters, vol. 18, no. 2, pp. 189–192, 2011.

[14] Y. Rachlin, and D. Baron, “The Secrecy of Compressed Sensing Measurements,” IEEE Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, vol. 52, pp. 813–817, 2008.

[15] M.R. Mayiami, B. Seyfe, and H.G. Bafghi, “Perfect Secrecy via Compressed Sensing”, IEEE Workshop on Communication and Information Theory (IWCIT), pp. 1- 5, 2013.

[16] A.V. Sreedhanya, and K.P. Soman, “Ensuring Security to the Compressed Sensing Data Using a Steganographic Approach,” International Journal of Advances in Image Processing, vol. 3, no. 1, pp. 1–7, 2013.

[17] C. Hung Chuang, and G. Shiang Lin, “The Optical Image Cryptosystem with a Position Selected Data Embedding Technique,” Proceedings of National Computer Symposium (NCS), vol. 3, pp. 531–536, 2007.

[18] 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, vol. 42, no. 8, pp. 2331–2339, 2003.

[19] W. Chung Kuo, “Data Hiding Method with High Embedding Capacity Character,” International Journal of Image Processing (IJIP), vol.3, no.6, pp. 310–317, 2010.

[20] M. Amin, “A Steganographic Method Based on DCT and New Quantization Technique,” International Journal of Network Security, vol.16, no.4, pp. 265–270, 2014.

[21] M. Khodaei and K. Faez, “New Adaptive Steganographic Method using Least Significant-Bit Substitution and Pixel-Value Differencing,” IET Image Processing, vol. 6, no. 6, pp. 677–686, 2012.

[22] T. Blumensath and M. E. Davies, “Sampling Theorems for Signals from the Union of Finite-Dimensional Linear Subspaces,” IEEE Transaction of Information Theory, vol. 55, no. 4, pp. 1872–1882, 2009.

[23] R. G. Baraniuk, “Compressive Sensing,” IEEE Signal Process Magazine, vol. 24, no. 4, pp. 118–120, 124, 2007.

[24] E. J. Candes, “Compressive Sampling,” International Congress of Mathematicians, vol. 3, pp. 1433–1452, 2006.

[25] E. J. Candes and M. B. Wakin, “An Introduction to Compressive Sampling,” IEEE Signal Process Magazine, vol. 25, no. 2, pp. 21–30, 2008.

[26] M. Duarteand Yonina and C. Eldar, “Structured Compressed Sensing: From Theory to Applications,” IEEE Transactions on Signal Processing, vol. 59, no. 9, pp. 4053–4085, 2011.

[27] J.A. Tropp and S.J. Wright, “Computational Methods for Sparse Solution of Linear Inverse Problems,” Proceedings of the IEEE, vol. 98, no. 6, pp. 948 –958, 2010.

[28] G. Davis, S. Mallat, and M. Avellaneda, “Adaptive Greedy Approximations,” Constructive Approximation, vol. 13, no. 1, pp. 57–98, 1997.

[29] D. Needell and J. A. Tropp, “CoSaMP: Iterative Signal Recovery from Incomplete and Inaccurate Samples,” Applied and Computational Harmonic Analysis, vol. 26, no. 3, pp. 301–321, 2008.

[30] B. Thomas, “Accelerated Iterative Hard Thresholding,” Signal Processing of Elsevier, vol. 92, no. 3, pp. 752–756, 2012.

[31] E. Candes and J. Romberg, “L1-Magic: Recovery of Sparse Signals via Convex Programming,” URL: www. acm. caltech. edu/l1magic/downloads/l1magic. Pdf4, 2005.

[32] T. Hale, W. Yin and Y. Zhang, “A Fixed –Point Continuation Method for– Regularized Minimization with Applications to Compressed Sensing,” Department of

Computer in Application Mathematical in Rice University, CAAM Technical Report TR07-07, pp. 1- 45, 2007.

[33] F. Vivek, S. Jagabathula and D. Shah "Sparse Choice Models," IEEE, 46th Annual Conference on Information Sciences and Systems (CISS), pp. 1–28, 2012.

[34] I. Venkata Sai Manoj and B. Tech, "Cryptography and Steganography," International Journal of Computer Applications, vol. 1, no. 12, pp.63–68, 2010.

[35] H.C. Andrews and C.L. Patterson, "Singular Value Decomposition (SVD) Image Coding," IEEE Transaction on Communications, vol. 24, no. 4, pp. 425–432, 2002.

[36] H. A. Abdallah, "An Efficient SVD Image Steganographic Approach," International Conference on Computer Engineering & Systems (ICCES), pp. 257–262, 2009.

[37] G. Jyothish Lal, V. K. Veena and K. P. Soman, "A Combined Crypto-Steganographic Approach for Information Hiding in Audio Signals Using Sub-band Coding, Compressive Sensing and Singular Value Decomposition," Springer Berlin Heidelberg, Communications in Computer and Information Science, vol. 377, pp. 52–62, 2013.

[38] P. Baoand Max, "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 15, no. 1, pp. 96–102, 2005.

[39] F. Petitcolas, R. Anderson, and M. Kuhn, "Information Hiding – a Survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.

[40] S.A. Laskar and K. Hemachandran, "High Capacity Data Hiding using LSB Steganography and Encryption," International Journal of Database Management Systems (IJDMS), vol.4, no.6, pp. 57–68, 2012.

[41] B. E. Carvajal–Gámez, F. J. Gallegos–Funes and J. L. López–Bonilla, "Scaling Factor for RGB Images to Steganography Applications," Journal of Vectorial Relativity, vol. 4, no. 3, pp. 55–65, 2009.

[42] G. Ulutas, M. Ulutas and V. Nabiyev, "Distortion Free Geometry Based Secret Image Sharing," Procedia Computer Science, vol.3, pp. 721–726, 2011.

Authors' Profiles

Fatemeh Kafash Ranjbar received BSc degree in communication from Industrial University Sajad in 2013, and her MSc in communication from Islamic Azad university, south Tehran branch in 2016. She is currently working in electrical industry in Iran. Her research interest is signal processing, image processing and secure telecommunication.

Sedigheh Ghofrani received her Ph.D. from Iran University of Science and Technology in 2004. She is associate professor since 2012. Her area of research includes image processing and signal processing. In 2003, she spent eight months at the School of Electronic and Electrical Engineering, the University of Leeds, UK, supported by British Council foundation. In 2012, she spent eight months at the Center for Advanced Communications (CAC) at Villanova University, PA, USA, as visiting research professor.

How to cite this paper: F. Kafash Ranjbar, S. Ghofrani,"Evaluation Compressive Sensing Recovery Algorithms in Crypto Steganography System", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.8, No.10, pp.53-63, 2016.DOI: 10.5815/ijigsp.2016.10.07