Steganography with Projection aided Payload Dimension Reduction and Reconstruction for Military Covert Communication

Ratnakirti Roy
Department of Computer Applications
National Institute of Technology
Durgapur, India

Suvamoy Changder
Department of Computer Applications
National Institute of Technology
Durgapur, India

ABSTRACT
Steganography techniques find importance in military applications because of their ability to communicate covertly. It is evident for any image steganography technique that if the payload can be represented in a smaller dimension than its original form, then the actual embedding requirement can be lessened thereby improving the statistical imperceptibility of the method. This paper presents an image steganography technique specifically aimed to be used for military covert communication which utilizes payload dimension reduction using parallel beam projection of images. Efforts have been given to ensure that the proposed technique conforms to high Imperceptibility and Fidelity which are the primary quality requirements for any image steganography system.

Keywords
Steganography, Image Steganography, Parallel Beam Projection, Radon transform, Image Reconstruction.

1. INTRODUCTION
In the recent years, the use of internet services has become more pervasive and affordable than ever before. Despite the role of internet as an excellent worldwide publicized medium for data transmission and sharing, confidentiality of information over the internet demands a lot more. Sensitive military data over networks may be stolen, intercepted, illegally modified, anonymized [1] or even destroyed by enemy intelligence resulting in data loss, leakage and damage. To preserve the privacy and confidentiality of sensitive military data over a computer network, it may be enclosed in a metaphorical envelope such that its contents are revealed only to the intended receiver. Data hiding techniques such as steganography aims at performing this task.

Steganography hides data into innocuous objects such that the very existence of the hidden data is imperceptible to an adversary [2]. Steganography proves useful in situations where public use of cryptography is either restricted or not allowed at all [3, 4, 5]. This makes steganography useful in military applications where covert communication is necessary to avoid enemy intelligence.

Given the fact that the statistical imperceptibility of a steganography technique is enhanced if the payload size is reduced [6], it is a good idea to devise a technique to reduce the dimensions of the payload without affecting the payload content drastically. Many steganography techniques [7, 8, 9, 10] that use compression can reduce the file size of the payload but not the pixel count if the payload is an image. For example, if an A×B image is the payload and it is subjected to compression techniques, the resultant payload still has its dimension or pixel count unchanged even though the file size is reduced. As an alternative, a reversible reduction mapping capable of regenerating the payload in presence of a suitable decoding key can be considered to be a viable solution. Steganography techniques using map based realization are termed as Image Realization Steganography [11, 12]. Parallel beam projection [13] of an image payload is observed to fulfill the requirements of such a mapping scheme.

The current work derives its motivation from X-ray computed tomography [14]. The basic problem of tomography is, given a set of 1-D projections and the angles at which these projections were taken, how do we reconstruct the 2-D image from which these projections were taken [15]? The projection data is generated as a result of multi-angle scan of a subject. It is then reconstructed to give back a combined 2D visualization enabling a medical practitioner to diagnose the patient accurately. The reconstruction or back projection [16] is of particular interest in the current research. The number of angles involved in scanning procedure determines the size of the projection data. Therefore, if a smaller sized projection equivalent of a payload image can be generated, then it will be sufficient to reconstruct the original payload. This is advantageous for application in image steganography because the projection data can be sized to be smaller than actual payload thereby reducing the actual embedding requirement. Similarly, the generated projection data does not bear any observable resemblance with the actual payload but can regenerate the payload on being supplied with appropriate parameters. Therefore, the feature can be considered to be important for payload security.

This paper aims to propose an image steganography technique intended for military covert communication. The proposed technique does not hide the actual payload directly in a cover image but hides its reduced projection equivalent map instead. The embedded information can regenerate the actual payload only in the presence of an exact decoding key.

2. PARALLEL BEAM PROJECTION
Parallel beam projection of a grayscale image can be implemented using the Radon Transform [17]. At any angle $theta(\theta)$, the projection over an image *f(x, y)* is as given in Fig 1 [18].

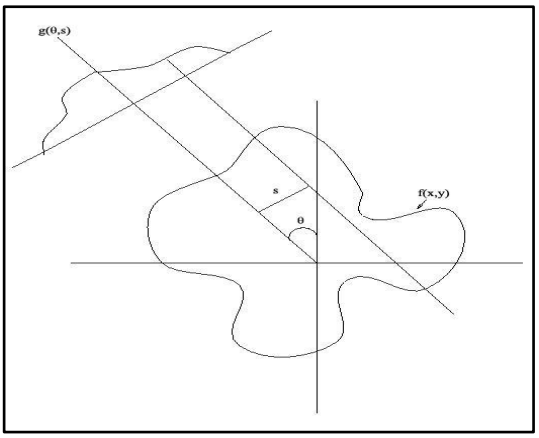

Fig 1: Projection of an image at a given angle

The Radon Transform over an image *f(x,y)* is defined as follows: Let $g(\theta, s)$ be a one dimensional projection at an angle θ. $g(\theta, s)$ is then the line integral of the image pixel *f(x,y)* along a line *z* which is at a distance *s* from the origin and at angle θ off the x-axis. Therefore,

$$g(\theta, s) = \int_z f(x, y)dz \qquad (1)$$

All points on the line denoted by Eqn. (1) satisfy the equation:

$$xsin\theta - ycos\theta = s \qquad (2)$$

Eqn. (1) can then be re-written as:

$$g(\theta, s) = \iint f(x, y)\delta(xsin\theta - ycos\theta - s)dxdy \qquad (3)$$

The collection of these $g(\theta, s)$ at all θ is called the Radon Transform of image *f(x, y)*. An example showing an image and its parallel beam projection data using Radon Transform is shown in Fig 2. It is clear from the figure that number of pixel in the projection equivalent is less than that in the original image.

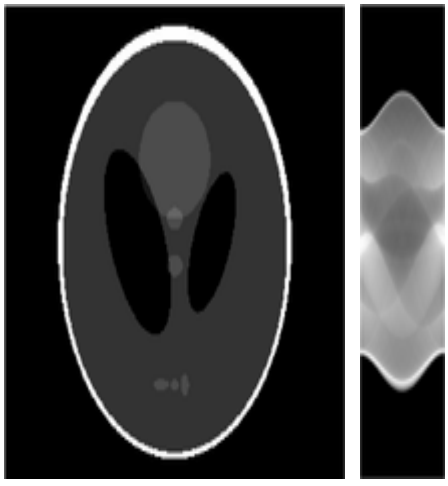

Fig 2. Shepp-Logan Phantom [20] and its Radon Transform

***Input**:* A cover image *C*, secret image *M*.

***Output**:* Stego image *S*

Algorithm:

Step 1: Apply Radon transform on *M* to generate the parallel beam projection data *P*.

Step 2: Convert *P* to its binary equivalent vector *B*. Calculate *L=|B|*.

Step 3: Calculate the number of pixels needed for embedding. Let this be denoted by *pixnum*. Set *pixnum:=L/2*.

Step 4: Set *P_set:=PRNG(pixnum) //Seed the Pseudo-random number generator to generate target pixel list*

Step 5: Set a counter *i*. Set *index=1*.

For *i:=1 to pixnum*

1. Set *pix*:=i^{th} pixel values from the set of pixels selected in *P_Set*.
2. Let *a1*=Red Plane LSB of *pix*, *a2*=Green Plane LSB of *pix*, *a3*= Blue Plane LSB of *pix*.
3. Let *x1=B (index)*, *x2=B (index+1)*.
4. Perform Embedding using operations conforming to Eqn. 6. Restore the original pixels with the changed pixel values wherever necessary.
5. Set *index=index+2*.

End For

Step 6: Write the modified image matrix to generate *S*.

Algorithm 1: Embedding Procedure

***Input**:* Stego Image *S*, Stego key *K*

Output: Secret Message *M*

Algorithm:

Step 1: Decode *K* to regenerate the actual payload reconstruction parameters, length of the embedded message *L*.

Step 2: Calculate number of pixels to search for hidden data as *pixnum:=L/2*.

Step 3: Set a counter *i, M'*:=[ ].

For *i:=1 to pixnum*

1. Set *pix*:= i^{th} pixel values from the set of pixels supplied as decoding information.
2. Let *a1*=Red Plane LSB of *pix*, *a2*=Green Plane LSB of *pix*, *a3*= Blue Plane LSB of *pix*.
3. Perform XOR operation on *a1* and *a3* to get the first message bit *x1*. Perform XOR operation on *a2* and *a3* to get the second message bit *x2* hidden in the pixel.
4. $M' := concat(M', x1, x2)$;

End For

Step 4: Set $M := reshape(M', p' * q')$;

Step 5: Apply Inverse Radon Transform on *M*.

$$M = reshape\ (M, p * q);$$

Step 6: Return *M*.

Algorithm 2: Extraction Procedure

3. THE PROPOSED MECHANISM

The proposed mechanism works in the spatio-transform domain and uses a parallel beam geometry based payload dimension reduction process to minimize the embedding requirement. Embedding is done on a pseudo-random pixel sequence to enhance imperceptibility. A stego key is also incorporated to protect the payload. In a further effort to reduce the number of bits that needs to be overwritten, the proposed technique employs *Matrix Encoding* [19], a high efficiency embedding scheme based on syndrome codes and capable of minimizing the embedding impact. The scheme is represented using a triplet (F, g, k) where each k bits of the secret message is embedded into g cover bits with at most F bit changes. Mathematically, the embedding function (*Emb)* and the extraction function (*Ext)* for any message $g \in \mathcal{M}$ is as follows:

$$Emb: \{0,1\}^n \mathcal{M} \rightarrow \{0,1\}^n, Ext: \{0,1\}^n \rightarrow \mathcal{M} \quad (4)$$

such that for all $g \in \mathcal{M}, k \subseteq g$ and any cover $x \in \{0,1\}^n$,

$$Ext\big(Emb(x,g)\big) = g \quad (5)$$

$$d\big(x, Emb(x,g)\big) \leq F \quad (6)$$

where, *d(.)* implies the change rate. The proposed system uses the matrix embedding *(1,3,2)* scheme, that is, for every three bits in the cover image, two message bits are embedded making at most one change at a time. A simple LSB based system overwrites only 50% of the available LSBs [4] whereas Matrix Encoding has an embedding density of 25% 17. It therefore embeds the same number of bits with less number of bit overwriting.

The proposed technique comprises of two phases. The first deals with the actual data embedding and key generation, while the second phase is concerned with the extraction of secret data.

3.1 Embedding Algorithm

The embedding algorithm uses a radon transform based parallel beam projection map of the actual image payload as the to-be-embedded information. Once the embedding is complete, the generated stego file can be sent to the receiver with the decoding information. The embedding procedure is elaborated in Algorithm 1.

3.2 Key Generation

The key generation is an important process in the design of any steganography system. In the current context, the stego key K is produced by a reversible hash function $\varphi(.)$ by combining different parameters related to extraction of the secret message. The key generation procedure is explained next.

Let, the secret message length (binary bit string) = l,

Secret image dimension = $p \times q$

Dimensions of the transform equivalent of secret message = $p' \times q'$

Number of angles required to reconstruct the secret image = ε

Pseudo Random Number Generator seed = ∂

The hash function $\varphi(.)$ takes $p, q, p', q', l, \varepsilon, \partial$ as inputs and combines them using such that,

$$K = \varphi(p, q, p', q', l, \varepsilon, \partial)$$

And,

$$[p, q, p', q', l, \varepsilon, \partial] = \varphi^{-1}(K)$$

The combination is performed using integer pairing [21, 22]. Integer pairing works as follows:

Let $\mathbb{Z}^+ = \{0,1,2\ldots\}$ be the set of non-negative integers and let $\mathbb{Z}^+ \times \mathbb{Z}^+$ be the set of all ordered pairs of non-negative integers. Then a quadratic bijection which maps $\mathbb{Z}^+ \times \mathbb{Z}^+$ injectively onto $\mathbb{Z}^+$ can be defined as:

$$\aleph = C(\rho, \tau) = \frac{1}{2}(\rho + \tau - 2)(\rho + \tau - 1) + \rho \quad (7)$$

where $\rho, \tau \in \mathbb{Z}^+$. Eqn. (7) computes an integer corresponding to an integer pair (ρ, τ). The generated value $\aleph$ can be again decomposed giving the original pair. Let,

$$\lambda = \left\lfloor \sqrt{2\aleph} - \frac{1}{2} \right\rfloor \quad (8)$$

$$\Delta\lambda = \frac{1}{2}\lambda(\lambda + 1) \quad (9)$$

Using Eqns. (8-9), ρ and τ are regenerated as:

$$\rho = \aleph - \Delta\lambda$$

$$\tau = \lambda - \rho + 2$$

In the current context, integer pairing is used in a chained combinational manner as:

Let,

$$\boldsymbol{\mu_1} = C(p, q), \boldsymbol{\mu_2} = C(p', q'), \boldsymbol{\mu_3} = C(\mu_1, \mu_2)$$

$$\boldsymbol{\mu_4} = C(\mu_3, l), \boldsymbol{\mu_5} = C(\mu_4, \varepsilon), \boldsymbol{\mu_6} = C(\mu_5, \partial)$$

$$\boldsymbol{SK_1} = C(\mu_1, \mu_2), \boldsymbol{SK_2} = C(\mu_3, \mu_4)$$

$$\boldsymbol{SK_3} = C(\mu_5, \mu_6)$$

$$\boldsymbol{K_1} = C(SK_1, SK_2)$$

$$\boldsymbol{K} = C(K_1, SK_3)$$

K is the final output stego key and the hash function $\varphi(.)$ performs all the above calculations and generates K. Keys generated using such a combination approach can be proved to have a key space large enough to resist *Brute Force* attacks for a considerable amount of time.

3.3 Extraction Algorithm

The extraction algorithm takes the stego image S and the stego key K as the input and extracts the hidden data using the decoding information available from the key. The extraction algorithm is explained as in Algorithm 2.

4. EXPERIMENTAL RESULTS AND ANALYSIS

The technique proposed in the previous section has been implemented in MATLAB 2013a and tested on a 32-bit 2.4 GHz single core processor computer. The cover images used were of lossless image format and selected from a standard image database (*USC-SIPI Image Database available at: http://sipi.usc.edu/database/).* The payload used was the standard grayscale *Elaine* image of different sizes. The algorithm was tested for the level of visual *fidelity*, *visual* and *statistical imperceptibility*) and the *degree of payload dimension reduction* due to adoption of parallel beam projection of the payload. Some of the images from the aforesaid database that are used as covers are shown in Fig 3.

Fig 3: Sample Cover Images

4.1 Measuring the Embedding Distortion

The distortion produced in the cover image due to the embedding is measured in terms of *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR).* Higher *PSNR* value indicates better fidelity of the image which in turn signifies lower visible distortion. *PSNR* value is expected to be greater than 40 *dB [4]* for high fidelity stego image.

Table 1. Distortion Measure for Various Levels of Embedding

Payload	*Nadal*		*Baboon*		*Landscape*	
	MSE	*PSNR (dB)*	*MSE*	*PSNR (dB)*	*MSE*	*PSNR (dB)*
64 x 64	0.0027	69.43452	0.0028	69.11864	0.0029	68.81384
70 x 70	0.0041	65.80612	0.0045	64.99755	0.0046	64.80664
80 x 80	0.0065	61.80353	0.0061	62.3552	0.0063	62.07499
100 x 100	0.0094	58.59924	0.0098	58.23728	0.0099	58.1491
110 x 110	0.0107	57.47412	0.01075	57.43363	0.0108	57.39332
128 x 128	0.0111	57.15534	0.0110	57.23395	0.0115	56.84784

The results in Table 1 indicate that the proposed algorithm produces high *PSNR* even at moderately high embedding rates for different covers. In all the cases, the *PSNR* is greater than the human visual threshold of 40 *dB* thereby producing high fidelity visually near perfect stego images.

4.2 Histogram Analysis for Imperceptibility

The frequency histogram of the sample cover image (*Nadal*) and the stego image generated after the embedding is presented in Fig 4. The top and the bottom rows show the frequency histogram of the cover image and the stego image respectively for each of the colour channels (Red, Green and Blue). Careful observation reveals that the two sets of histograms vary negligibly in the red, green and the blue planes (Sample variations are marked using circles) signifying high visual fidelity.

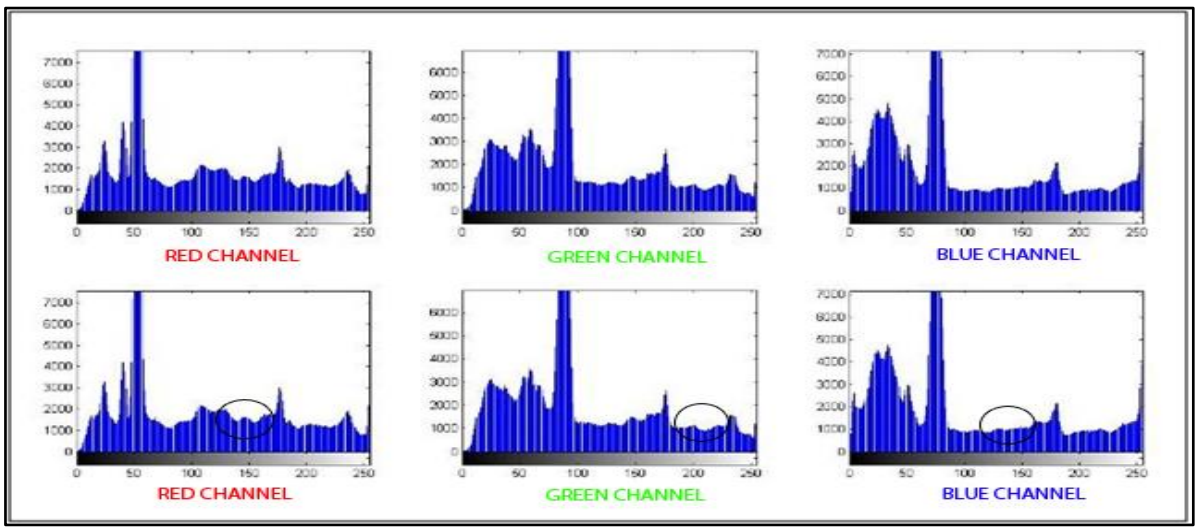

Fig 4. Histograms of the Sample Cover (top) and Stego (bottom) images

4.3 Sensitivity to steganalysis tests

In order to assess the degree of statistical imperceptibility offered by the proposed technique, the stego images generated were subjected to χ^2-attack [23]. The results are shown in Table 2.

Table 2. Sensitivity to steganalysis test

Payload Size	*Probability of Embedding(approx. Rounded values)*		
	Nadal	*Mandrill*	*Landscape*
64 x 64	0.0001027	0.00010	0.0001025
70 x 70	0.000103	0.000101	0.0001024
80 x 80	0.0001301	0.0001025	0.0001027
100 x 100	0.0001305	0.0001025	0.00011

It is evident from the results that the probability of embedding as generated from the χ^2-attack is extremely low (not greater than 0.0002). Such figures clearly suggest the effectiveness of the proposed technique in resisting common statistical attacks.

4.4 Payload Dimension Reduction

Payload dimension reduction is one of the key features of the proposed technique. Sample image payload, their projection data and the reconstituted image is shown in Fig 5, 6 and 7 respectively. Table 3 reveals that the projection data of the actual image payload is smaller in dimension than the original payload. This however depends on the number of angles which are taken into consideration while generating the projection data. Such a reduction in the dimension is beneficial as it reduces the embedding requirement. Merging payload dimension reduction scheme with a high efficiency embedding technique ensures that the distortion produced in the cover due to embedding is minimized.

Table 3. Payload Reduction Data

Original Dimension of payload(α)*	*Projection Equivalent Dimension of payload(α')*	*Number of Angles(θ)*	*Difference in dimension(pixels)* $[\alpha - \alpha']$
64 x 64	95 x 18	18	2386
70 x 70	103 x 36	36	1192
80 x 80	117 x 36	36	2188
100 x 100	145 x 68	68	140
110 x 110	159 x 75	75	175
128 x 128	185 x 90	90	266
**: Dimension refers to the number of pixels*			

Fig 5: Image Payload

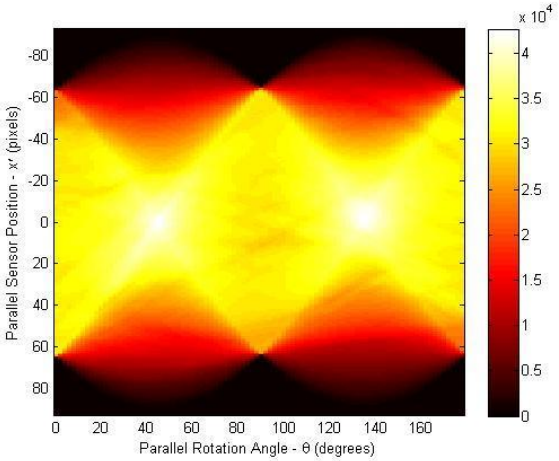

Fig 6: Parallel Beam Projection Equivalent (Color Map Used)

Fig 7. Reconstructed Image

5. COMPARATIVE ANALYSIS

The performance of the proposed scheme is compared with other techniques (with similar test environment) with respect to the following parameters: *Visual Fidelity*, *Payload Dimension Reduction* and *Payload Security*. The results are tabulated in Table 4.

Table 4. Comparative Analysis

Method	*Average PSNR(dB)*	*Payload Dimension Reduction*	*Additional Payload Security*
Goel *et al.* [7]	48.6	LZW	Nil
Thangalatha *et al.*[8]	53.27	Z-Transform	Nil
Tang *et al.* [9]	32.64 (Max.)	AMBTC	Nil
Guo *et al.* [10]	40.0625	JPEG Double Compression	Nil
Proposed Method	61.5403	Radon-Transform based projection	*Key based*

The results indicate that the proposed method outperforms similar other techniques both in terms of visual fidelity and payload security. This clearly indicates the effectiveness of the reduction technique, embedding method and the key based payload security scheme adopted in the proposed method.

6. CONCLUSION AND FUTURE WORK

This paper presents an image steganography technique that uses a payload dimension reduction by parallel beam

projection of the image payload. The projection data is embedded into the cover, coupled with a high efficiency embedding scheme. Experimental results on grayscale payload validate that the payload dimension reduction significantly lessens the embedding requirement resulting in high fidelity stego image and minimal variation histograms. The technique can be easily extended for colour image payload with appropriate modifications.

However, the parallel beam projection of the image payload depends on the number of angles considered for the transformation. Therefore, it is important to exercise caution in choosing the angular range so as to guarantee optimal quality of the extracted payload.

Future work will concentrate on studying the possibility of applying other image reconstruction methods for the design of more efficient image steganography techniques.

7. REFERENCES

[1] Kelly, G. & McKenzie, B. *Security, privacy and confidentiality issues on the internet*. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761937/ [Accessed on 3rd June, 2015].

[2] Morkel, T.; Eloff, J.H.P.; Olivier, M.S. *AN OVERVIEW OF IMAGE STEGANOGRAPHY*. In Proc. Fifth Annual Information Security South Africa Conference (ISSA2005), 2005.

[3] Koops, Bert-J. *Overview per country. Crypto Law Survey*.2013. http://www.cryptolaw.org/cls2.htm [Accessed on 20th June, 2015]

[4] *What are the Cryptographic Policies of Some Countries?* http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/cryptographic-policies-countries.htm [Accessed on 15th June, 2015].

[5] Serdean, C.V.; Tomlinson, M.; Wade, J.; Ambroze, A.M. *Protecting Intellectual Rights: Digital Watermarking in the wavelet domain*. In Proc. IEEE Int. Workshop Trends and Recent Achievements in IT, 2002, pp. 16-18.

[6] Ahmed, D.E.M.; Khalifa, O.O. *Robust and Secure Image Steganography Based on Elliptic Curve Cryptography*. In Proc. 2014 International Conference on Computer and Communication Engineering (ICCCE), 2014, pp. 289-291. doi: 10.1109/ICCCE.2014.88

[7] Goel, S.; Kumar, P.; Saraswat, R. *High Capacity Image Steganography Method Using LZW, IWT and Modified Pixel Indicator Technique*. IJCSIT, 2014, 5(3), 3759-3763, ISSN: 0975-6946.

[8] Thangalatha Legaz, C.; Nivetha, K, Saranya, R., Mathumathi, V. *Image Hiding with Payload Reduction using Z-Transform Steganography*, IJERT, 2014, 3(4), 866-869, ISSN: 2278-0181.

[9] Tang, M.; Zeng, S.; Chen, X.;Hu, J.;Du, Y. *An adaptive image steganography using AMBTC compression and interpolation technique*. Optik - International Journal for Light and Electron Optics, 2016, 127(1), 471-477, Elsevier B.V, DOI: doi:10.1016/j.ijleo.2015.09.216.

[10] Guo, J.-M.; Thanh, N.L. *Secret Communication Using JPEG Double Compression*, IEEE Signal Processing Letters, 2010, 17(10), 879-882, doi: 10.1109/LSP.2010.2066110.

[11] Samima, S.; Roy, R.; Changder, S. *Secure Key based Image Realization Steganography*. In Proc. IEEE International Conference on Image Information Processing(ICIIP 2013), Shimla, December 2013, pp. 377-382.

[12] Roy, R. & Changder, S. *Image Realization Steganography with LCS based Mapping*. In Proc. 7th International Conference on Contemporary Computing (IC3 2014), August 2014, pp. 218-223.

[13] Cierniak, R. *Reconstruction from Parallel-beam Projections. X-Ray Computed Tomograph*y. In Biomedical Engineering, 2011, Springer London, pp. 83-125.

[14] *X-Ray Computed Tomography*. http://en.wikipedia.org/wiki/Xray_computed_tomography [Accessed on 7th January, 2015].

[15] *Image Projections and the Radon Transform*. https://www.clear.rice.edu/elec431/projects96/DSP/bpanalysis.html [Accessed on 14th December, 2014].

[16] Smith, Steven W. *Special Imaging Techniques*. Digital Signal Processing: A Practical Guide for Engineers and Scientists, 1st Edition, 2002, Newnes, Chapter 25.

[17] Megherbi, N.; Breckon, T.P.; Flitton, G.T.; Mouton, A. *Radon Transform based Metal Artefacts Generation in 3D Threat Image Projection*. In Proc. SPIE Optics and Photonics for Counterterrorism, Crime Fighting and Defence, 2013, pp.1-7.

[18] *Tomographic Reconstruction*. http://en.wikipedia.org/wiki/Tomographic_reconstruction [Accessed on 8th January 2015].

[19] Crandall, R. *Some Notes on Steganography*. Steganography Mailing List, 1998. http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0203/steganografia/LINKS%20LOCALI/matrix-encoding.pdf [Accessed on 19th December, 2014]

[20] Shepp, L. & Logan, B.F. *The Fourier Reconstruction of a Head Section*. IEEE Transactions on Nuclear Science, 1974, 21(3), 21-43.

[21] Szudzik, M., *An Elegant Pairing Function*. http://szudzik.com/ElegantPairing.pdf [Accessed on 22nd June, 2015]

[22] Cantor, G., A Contribution to the Theory of Manifolds, Journal of Pure and Applied Mathematics, 1878, 84, 242-258 (German).

[23] Provos, N. & Honeyman, P. Hide and Seek: An Introduction to Steganography. IEEE Security and Privacy, 2003, 1(3), 32-44.