

# A Novel Data Hiding Framework Using Switching Threshold Mechanism

Saurabh Agrawal, J. S. Yadav, Ravindranath C. Cherukuri

**Abstract**— In the current digital era, the rapid escalations in digital multimedia and network have paved ways for people around to acquire, utilize and share multimedia information. In this paper, we introduce a novel algorithm for hiding significant amount of data while preserving the image artifacts. The algorithm uses image details and identifies the good locations for hiding using a discriminative filter. This principle enhances the immunity of the proposed system against stego detection algorithms and preserves the first order statistics of the image. In addition, the proposed algorithm could retrieve the embedded information without the prior information of the original cover. The simulation analysis would show that the proposed method offers higher immunity to stego detection algorithms and preserve the first order statistics of the image.

**Index Terms**—Information security and assurance, discriminative filter, switching mechanism, and steganography, secured communication.

## I. INTRODUCTION

In current digital era, an organization or country's advanced digital security systems could easily determine their global advancement. The potential digital communication channels have expanded into a realm of mass digital media. Digital carriers include e-mail, audio and video messages, disk space, disk partitions and image. With all the possible channels in existence today, data hiding may be classified as an entity of its own with wide range of latent applications [1].

Recently, data hiding techniques were quite effective exploited in digital media authentication, tracking and copyright protection. Steganography (in Greek literally means 'Covered Writing') is widely employed for sharing a secret information/message between two authorized users without revealing its presence to any of the third party viewers. Technically, it is an art of secret communication. Practically, data hiding can be viewed as a new kind of covert communication system, which is a combination of a communication and a multimedia covert system working in tandem to provide a secured digital transfer between the authorized users [2].

The key concept of steganography is to serve as a viable channel for communication while ensuring the transmission is not visible to the informal eye. In fact, the presence of

communication should only be realized by the sender and the recipient/recipients. Any steganographic method should possess the following properties [3]:

- Good visual & statistical imperceptibility for the security of hidden communication.
- Sufficient payload for ensuring that a large quantity of data can be conveyed.

The digital images are used as cover images to embed information in a concealed manner within the bits of the image. A simplest steganographic method involves the manipulation of the least significant bit (LSB) plane of the data. Various techniques, such as direct replacement of the cover's LSB with the information bits or an arithmetic combination between the two are used in several watermarking and steganography applications [4-5].

An approach proposed [6] in time domain, called *patchwork* that embeds depending on the statistics of the original image acted as base for several steganographic systems developed. In this approach, pairs of image regions are selected using a pseudorandom sequence initially. Once a pair is selected, the pixel intensities within one region are increased by a constant value while the pixels of the second region are correspondingly decreased by the same value. The modification is typically small and not perceptible, but is not restricted to the LSB. A texture mapping method that copies areas of random textures from one area of the image to another is also described.

In general, existing LSB embedding techniques can be classified into two classes namely: 1) Non-Adaptive embedding frameworks [7-8] and 2) Adaptive embedding frameworks. Non-adaptive data hiding frameworks focus on mere hiding information without preserving the image statistics. The hiding normally takes places in sequential manner or random walk process.

Unfortunately, Non-Adaptive embedding methods are simple to implement and offer high embedding capacity unfortunately there several drawbacks. These methods:

- do not consider the cover image features leading to embedding in regions where detection is likely.
- often embedded the stego data compactly in small region which in turn affects the first order statistics and
- easily detected by localized or simple statistics based stego detection algorithms.

Henceforth, due to the above limitations adaptive embedding has gained a significant research focus within the field of steganography. Further, we introduce a novel adaptive data hiding method that utilizes the image statistics for hiding multiple bits of information within a given cover image. The pixel selected of the image is carried could based on the median statistics of the image.

**Manuscript published on 30 June 2013.**

\* Correspondence Author (s)

Saurabh Agrawal, EC Department, MANIT, Bhopal, India.

Dr. J. S. Yadav, EC Department, MANIT, Bhopal, India.

Dr. Ravindranath C. C, EE Department, Gyan Ganga Institute of Technology and Management, Bhopal, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

The following paper has been organized as follows. In this correspondence, Section 2 describes about various existing adaptive techniques and the basic architecture of the block selection. Section 3 presents the new framework for classifying each image pixels into embeddable or non-embeddable pixels based on localized image statistics. The proposed system and its algorithm are explained in section 4 with detail illustrations. Section 5 deals with the experiments results and the security analysis of the algorithm. Section 6 concludes the paper.

### II. ADAPTIVE DATA HIDING

#### A. Adaptive Data Hiding

An adaptive data hiding framework is a process of inherently selecting cover pixels for hiding information whose change would not affect the localized neighborhood. The most important aspect of any adaptive system as it could improve the immunity against stego detection algorithm while hiding significant amount of digital information bits [2]. It is an ever evolving topic in the scientific field of adaptive steganography. There have been numerous adaptive frameworks based on various pixel selection algorithms have been proposed over the last few years.

One of the ways to evaluate the performance of these approaches is the embedding efficiency and the embedding capacity. Moreover, the immunity of the embedding approaches against various first-order statistical attacks plays a prominent role while selecting an approach. For example, an approach could offer a high embedding capacity but low embedding efficiency that would result in visual distortions in the cover. Similarly, if it offers high embedding capacity and high embedding efficiency but easily detected against the statistical attacks that reduce the demand for that algorithm. If these issues form three corners of triangle then a perfect steganographic algorithm would be at an optimum distance from each of the corners, i.e. center of the triangle.

#### B. Background

Niimi, Noda, and Kawaguchi [9] introduced an image-based steganographic technique which categorizes bit-planes blocks into “noise” or “informative” regions. The secret data is embedded into the noise blocks by altering a set of values and the remaining values are used for adjusting the complexity measure. Elke Franz [10] introduced a more rigorous approach for hiding secured information that concentrated on retaining first and second order statistics when embedding the cover image with stego data. Histogram frequencies are maintained by modeling the embedding process as a Markov source and modifying the information to be embedded so that it resembles the ideal distribution pertaining to the cover image. D.C Wu and W.H Tsai proposed [11] the pixel-value differencing technique that segments the cover into non-overlapping blocks containing two connecting pixels. The pixel difference of those is modified for data embedding. There are two limitations generally associated with adaptive embedding techniques: 1) a limited embedding capacity for a given cover, 2) methods resistant to one detection method are vulnerable to others variant in nature.

S. Aгаian, B. Rodriguez, and J. Perez [12] presented an embedding technique for palette images where a complexity measure was used to separate the image into embeddable and non-embeddable regions. In this approach the capacity of a particular block was determined by the resultant value of the presented complexity measure. S. S. Aгаian, R. R. Sifuentes,

and R. C. Cherukuri [13] proposed an additional perspective to adaptive steganography by suggesting a pixel focused approach. The algorithm was able to adaptively select the number of bits to embed per pixel using t-order statistical local characterization in order to find excessively noisy image regions where pixels could withstand changes of greater magnitude in order to embed multiple bits. In addition, a Pn-sequence based embedding technique is incorporated to hide the information in the selected bits.

In order to make steganography a more viable solution for secret communication, we must formulate a means for an increased embedding capacity and still ensure that the resultant message carrying image is still resistant to any attempts at detection. How can one improve the balance offset between security and capacity? In order to simultaneously enhance the embedding capacity and reduce any visual or statistical distortion in the cover image, an elaboration is formulated to further improve upon the benefits of the adaptive selection of the number of bits to embed per pixel needs to be addressed.

### III. LOCALIZED PIXEL SELECTION

The foundation of most adaptive embedding algorithms is the application of some manner of consideration to the specific cover media being used for embedding purposes. Image details are considered by the algorithm and good locations for embedding are selected based on local information gathered in the vicinity of a given cover pixel. Many approaches have been proposed using such local measures as variance, standard deviation, median-based variance, t-order statistics, as well as the number of unique pixel values within a given distance be selected [14]. The fundamental principle of adaptive steganography is to embed information in such a way that ensures changes made to a cover image remain below the natural noise threshold associated with digital imagery. The natural noise that normally present in an image is due to the following reasons. 1) due to light condition during which the image is taken, 2) due to the hardware employed to take the image and 3) due to the handling of device while taking the image. Acknowledging the principle of increased security when embedding in high variation regions, one would assume that embedding on the edges of an image would be the most secure approach. Further investigation has shown that with close inspection, embedded information on vertical and horizontal edges causes recognizable artifacts in the resultant stego image. Though edges are characterized by abrupt changes in intensity, they also have a distinct structure that should be acknowledged. In order to select the pixel that could be employed for hiding the secured information bit, all the pixel variation over possible directions are determined [15]. The horizontal and vertical variations of the pixels based on the neighborhood are determined. The diagonal variation associated has more directions and hence mathematically complex and vital in determining the overall variation. In general, additional weight is given to the diagonal variation to reduce the impact of horizontal and vertical variations over the pixel variation could be addressed. The prime variations that are considered in this paper is presented in the figure 1. Prior to intensity variation calculation the image is padded with the column-wise and row-wise on four sides of the image.

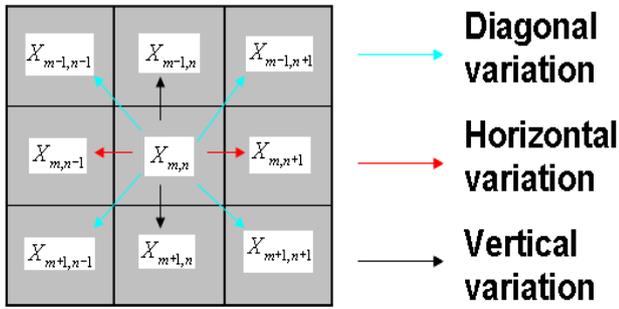


Fig.1. An image 3x3 block and variation that are employed in the selection pixel for hiding data

Let  $x_{mn}$  be the pixel under consideration at location  $(m, n)$  in an image of size  $M \times N$ .  $m=1, 2, \dots, M$ ; and  $n=1, 2, \dots, N$ . The variation intensity  $\hat{x}_{mn}$  may be defined as

$$\hat{x}_{mn} = \frac{\sqrt{(W_1 * V^2 + W_2 * H^2 + W_3 * D^2)}}{W_1 + W_2 + W_3} \quad \dots (1)$$

$\{W_1, W_2, W_3\}$  are the weights associated with vertical, horizontal and diagonal variations of the pixel and for simulation purpose equal weights for three variations are used. Further, the vertical, horizontal and diagonal variations of the pixels are calculated as shown below

$$H = \frac{\sqrt{(X_{m,n} - X_{m,n-1})^2 + (X_{m,n} - X_{m,n+1})^2}}{2} \quad \dots (2)$$

$$V = \frac{\sqrt{(X_{m,n} - X_{m-1,n})^2 + (X_{m,n} - X_{m+1,n})^2}}{2} \quad \dots (3)$$

$$D = \frac{\sqrt{D_1 + D_2}}{4} \quad \dots (4)$$

Where,

$$D_1 = (X_{m,n} - X_{m-1,n-1})^2 + (X_{m,n} - X_{m-1,n+1})^2$$

$$D_2 = (X_{m,n} - X_{m+1,n-1})^2 + (X_{m,n} - X_{m+1,n+1})^2$$

Thus estimated intensity measure of each pixel is incorporated in selection of the embeddable and non-embeddable pixels for secure hiding information bits. The embeddable pixels are further classified into multi-bit or single bit embeddable pixel. Further, multi-bit embeddable pixels are given high priority than the pixels with a single bit embeddable in terms of hiding information. In this paper, we limited to "2" bits in case of multi-bit embedding.

if  $\hat{x}_{mn} > \beta$  then the pixel is multi-bit embeddable pixel. If  $\beta > \hat{x}_{mn} > \alpha$  then the pixel is single bit embeddable pixel. And if  $\alpha > \hat{x}_{mn}$  then the pixel is a non-embeddable pixel.

Where,  $\alpha, \beta$  are threshold values that decide the capacity of the pixels in an image are determined based of weights of the bit-planes. The map corresponding to the cover image for hiding "1" secured bit and "2" secured bits is presented in the figure 2. In addition, we could also embed multiple bits by increasing the number of threshold values (i.e.  $\alpha, \beta, \gamma, \dots, \delta$ ). It is advisable to maintain a bit-plane weights difference between the threshold for security and statistical preservation of cover image.



Fig.2 a) Cover "Lena" red layer b) pixels in "Lena" that selected for hiding 1 bit c) Pixels in "Lena" that selected for hiding 2 bits  
The threshold value " $\alpha$ " is referred as the global threshold as it divides the whole image pixels into two classes i.e., embeddable and non-embeddable pixels. The threshold value " $\beta$ " is referred as the local threshold as it classify the embeddable pixels into single-bit or multi-bit carriers. The effect of local threshold and global threshold on the embedding capacity of the image is illustrated using the figure 3.

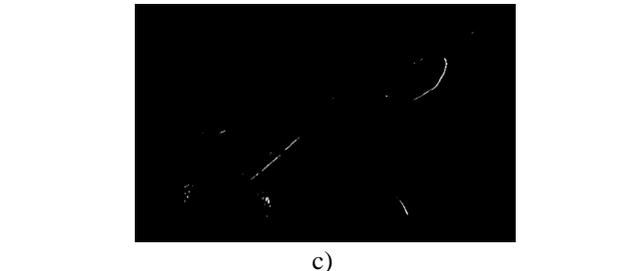


Fig.3. Comparison of the effect of local threshold and global threshold on the capacity of the image in consideration using proposed algorithm

#### IV. PROPOSED ALGORITHM

The encoding process is an extensive process with many decisions and evaluations to be made depending on the desired security and capacity. If computational resources and processing time are crucial considerations as in implementation within a mobile device, a straightforward application may be formulated with less flexibility. Figure 4 introduces a block diagram of the general structure of the encoding process.

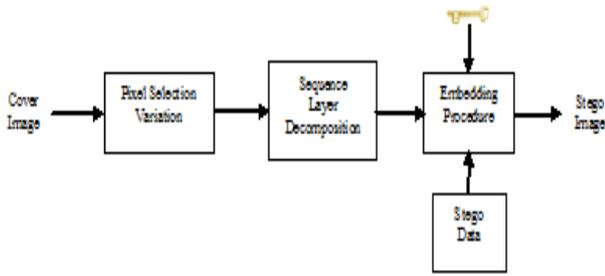


Fig.4. The general structure of encoding process of the proposed algorithm

**Cover Image.** The cover image may be of any image format using the 8-bit, power of two’s representation. Index images are to be included but with an additional pre-processing step of converting palette values into the RGB color space. The proposed algorithm may also be applied on 24-bit, three color layer images treating individual layers as an individual 8-bit image.

**Pixel Selection Variation.** The image is scanned and the presented variation measure is applied gauging the level of noise similarity within the proximal area of a given pixel. Again, horizontal and vertical edges are given less precedence while accentuating any diagonal edge power. Measure is assigned for all pixels and stored in memory.

**Sequence Layer Decomposition** Sequence code is selected and the number of least significant bit layers is selected based on the required capacity and the user’s security/capacity prioritization. The unique set of normalized sequence codes is formulated and the image is separated into binary layers.

**Embedding Procedure.** Key is constructed based on selected parameters and the size and format of the secret message. If message is an image, dimensions are included; if the message is a text file, then the number of characters is included; if message is an audio file, then number of samples is included; etc. Secret message is converted into binary representation and bits are incorporated into the least significant layers of the cover image. Image is reconverted back into decimal representation.

The decoding process is a straightforward process where all necessary parameters are dictated based on the size of the secret message. Pixel selection variation process is applied and image is decomposed into normalized sequence based bit layers based on the specified sequence code. Embedded bits are extracted and converted back into decimal representation. Secret message is then reconstructed.

V. COMPUTER SIMULATION

Computer simulations were simulated using MATLAB software package. Analysis was done using 100 color images of varying sizes, texture and contour. These images were taken using 2 digital cameras Nikon D100 and Canon EOS Digital Rebel and modified in Photoshop to attain a smooth histogram. In addition, for testing the capacity barriers of the proposed system varying sizes of embedding message are employed.

Initially, we test if the first order statistics of cover image are preserved before and after embedding data. The histogram comparisons of the stego images after hiding 25% (25% of size of the image) of data is embedded using various existing algorithms and proposed algorithm as presented in figure 5.

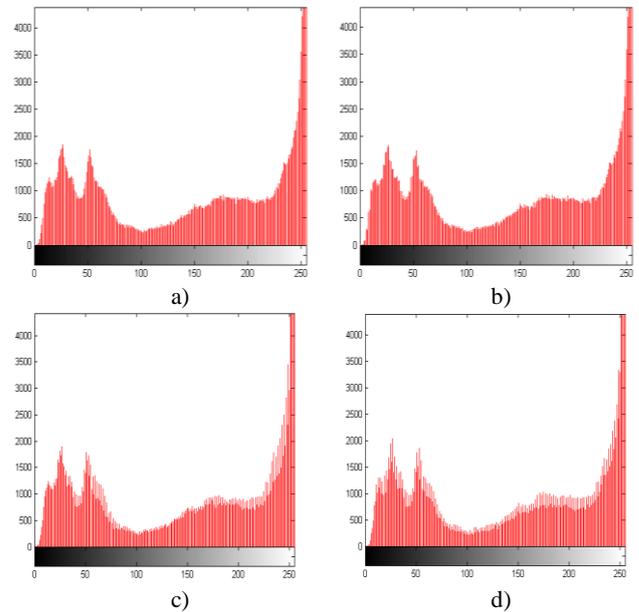


Fig.5. Histogram comparisons a) “Sarkis” image histogram before hiding information b) “Sarkis” image histogram after hiding 25% of data using proposed algorithm, c) “Sarkis” image histogram after hiding 25% of data using SecurEngine d) “Sarkis” image histogram after hiding 25% of data using lossless adaptive algorithm

The proposed method has proved to preserve the first order statistics of the cover image before and after embedding with reference to the common used existing methods like SecurEngine and lossless adaptive algorithm [16]. In addition, the visible image artifacts have also been preserved with the least visible distortion as presented in the figure 6.



Fig.6. Visible comparisons a) the original “Lena” before hiding any secured information b) “Lena” stego image after hiding 25% of secured data using proposed algorithm

Table 1 RS steganalysis attack – detected message length in number of bytes. 10%

	SecurEngine	Adaptive [17]	Non-Adap. [16]	New Method
Lena	6573	9363	12567	3041
Sarkis	3259	6355	11942	2314
House	3623	5244	10081	0
Insect	5453	3293	12330	279
Coast	5710	5538	12337	0
Flower	27775	27354	32055	23875
Collage	5137	5403	11528	514
Bonaza	18048	20184	23245	13628
Bouqee	6299	3156	11431	0



In the above test, we have established that the proposed algorithm could effectively preserve image artifacts and the first order statistics in comparison with the existing algorithms. In order to test the immunity of the proposed system, we test stego images after hiding 10% of the secured against RS steganalysis as discussed in the table 1. From table 1, we could establish that the proposed algorithm shows a prominent resistance to the steganalysis attack in comparison with the existing data hiding systems.

Further, consider the test image "House" of size 512x512 and a message about 10% of the cover is hidden using existing and proposed algorithms. RS steganalysis is performed over the stego image with information and results show that it could not detect the proposed algorithm where as other algorithms were detected. In case of the "Flower" and "Bonaza" images a clean cover was detected to have a significant amount of information. Further, in fact that detection from clean to stego image in case of "Bonaza" is reduced by 133 bits of information.

## VI. CONCLUSION

We introduced a novel algorithm for hiding significant amount of data while preserving the image artifacts. The proposed algorithm successfully identified the embeddable and non-embeddable pixels in the cover image based on a global threshold. Further, we have successfully classified multi-bit embeddable pixel to a single-bit based on a localized threshold. The combination of localized and global threshold could alter immunity, capacity and robustness of the algorithm. The simulation analysis has proved that the proposed method offers higher immunity against stego detection algorithms and preserves the first order statistics of the image simultaneously. Moreover, the proposed algorithm has retrieved the embedded information without the prior information of the original cover.

## REFERENCES

- [1] N. F. Johnson, Z. Duric, S. Jajodia, *Information Hiding Techniques Steganography and Watermarking Attacks and Countermeasures (Advances in Information Security)*, Springer Publishers, ISBN 1461369673, 2012
- [2] Ching-Nung Yang, Chia-chen Lin, Chin-Chen Chang, *Steganography and Watermarking*, Nova Science Publishers Inc., 2013
- [3] Ravindranath C. Cherukuri and Sos S. Aгаian, "New normalized expansions for redundant number systems: adaptive data hiding techniques", *Proceedings of SPIE on Multimedia on Mobile Devices 2010*, Vol. 7542, San Jose, California, USA 2010
- [4] Mamta Juneja, Parvinder Singh Sandhu, "Information Hiding Using Improved LSB Steganography and Feature Detection Technique", *International Journal of Engineering and Advanced Technology (IJEAT)*, Vol. 2, Issue-4, April 2013, pp.275-279
- [5] Shailender Gupta, Ankur Goyal and Bharat Bhusan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," *I. J. Modern Education and Computer Science*, 2012, Vol.6, pp-27-34
- [6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," *Journal of IBM Systems*, Vol. 35, 1996.
- [7] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems J.*, vol. 35, 1996.
- [8] WbStego, <http://wbstego.wbailer.com/>
- [9] S\_Tools, [http://bit599.netai.net/s\\_tools.htm](http://bit599.netai.net/s_tools.htm)
- [10] Niimi, M.; Noda, H.; Kawaguchi, E.; Eason, R.O., "Luminance quasi-preserving color quantization for digital steganography to palette-based images," *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, vol.1, no., pp.251,254 vol.1, 2002
- [11] Elke Franz. "Steganography Preserving Statistical Properties", *Information Hiding: 5<sup>th</sup> International Workshop, IH*. pp. 287-294. July 2003.
- [12] Wu, D.C.; Tsai, W.H., "Spatial-domain image hiding using image differencing," *IEE Proceedings in Vision, Image and Signal Processing*, vol.147, no.1, pp.29-37, Feb 2000.

- [13] Aгаian, S., Rodriguez, B., Perez, J., "Stego sensitivity measure and multibit plane based steganography using different color models", *IS&T/SPIE 18<sup>th</sup> Annual Symposium of Security, Steganography, and Watermarking of Multimedia Contents VIII*, February 2006, vol. 6072, pp. 279-290 (2006)
- [14] S.S.Aгаian, R.C.Chelukuri, S.Ronnie, "A New Secure Adaptive Steganographic Algorithm using Fibonacci Numbers", *2006 IEEE Region 5 Technology and Science conference*, San Antonio, USA, April 7-8 2006.
- [15] S. S. Aгаian, R. R. Sifuentes, R. C. Cherukuri, "T-Order Statistics and Secure Adaptive Steganography", *SPIE Optics & Photonics advance technical program*, San Diego, USA, 31July-4August 2005.
- [16] Chin-Chen Chang, Jun-Chou Chang, Yu-Chen Hu, "Spatial Domain Image Hiding Scheme Using Pixel-Values Differencing", *Fundamenta Informaticae*, Vol. 70, Issue-3, pp 171-184, 2006
- [17] Jessica. F; M. Goljan and R. Du, "Reliable Detection of LSB Steganography in Grayscale and Color Images" *Proceedings of the ACM Workshop on Multimedia and Security*, Ottawa, Canada, October 5, 2001, pp. 27-30

**Saurabh Agrawal** born on 25<sup>th</sup> July 1983. He received his degree in Electronics & communication from AMIETE New Delhi in the year 2006 and M.Tech from Maulana Azad National Institute of Technology (MANIT) Bhopal in 2009. Currently he is pursuing Ph.D from MANIT Bhopal in the area of Image Processing and Information assurance and security.

**Dr. J. S. Yadav** born on 30<sup>th</sup> June 1972. He received his B.Tech degree in Electronics & communication from R.D.V.V. Jabalpur in 1995, M.Tech from MANIT (Bhopal) in 2002 and Ph.D from MANIT(Bhopal) in 2011. Currently he is working as Associate professor in the department of Electronics & Communication MANIT Bhopal (M.P.). He worked in several organizations and has a vast 16 year of research & Teaching experience in Digital signal processing. He supervised more than 19 M.Tech Scholar and 5 Research Scholar. Currently he is the senior member of IACSIT (International Association of computer science and Information technology). He is also the Member of Human Right Commission to study the "Effect of Radiation from Mobile Tower". He is a Technical Expert for procurement of surveillance equipment, Anti-Terrorist Squad MP Police, Bhopal. He has published various research paper in reputed National and International Journal.

**Dr. Ravindranath C. Cherukuri**, born at Hyderabad (AP), India in 1981. He received his B.Tech degree in Electrical and Electronics engineering from JNTU, Hyderabad in 2002. He received his MS and Ph.D in Electrical and Computer Engineering from University of Texas San Antonio, in (2005 & 2011). He is the senior member of IACSIT, Life member of CRSI and Member various professional bodies. He is currently working in GGITM, Bhopal, India as Director Research Incubation Center and HOD Electrical and Electronics Department GGITM, Bhopal. His research interest includes System Security, Multimedia Processing, Information Assurance, and Applied Statistics. He has special interest in the development of secured systems and designs.