

An Invisible Communication for Secret Sharing against Transmission Error -A Steganographic Perspective

Rengarajan Amirtharajan, Vivek Ganesan, R Jithamanyu and John Bosco Balaguru Rayappan
Department of Electronics and Communication Engineering
School of Electrical & Electronics Engineering
SASTRA University
Thanjavur, Tamilnadu, India
amir@ece.sastra.edu

Abstract— The electronic and information revolutions have brought a plethora of sophistications to the today's world. Computer, one of the versatile inventions of human, always has more to offer to the benefit of the planet. The electronic substitutions to the five senses of humans have unveiled many unknown possibilities of harnessing the power of computers. The security of information handled in real time transmission and reception like internet is of paramount consideration, as this information may be confidential. This paper proposes a novel solution for handling of confidential information in real time systems, using a modern steganographic approach instead of conventional cryptographic methods. The proposed solution brings down the required channel capacity to transfer secret data in real time systems besides improving security.

Keywords- Information security; Steganography; Modified Least significant embedding(LSB);

I. INTRODUCTION

Information, the most sought after commodity of electronic epoch, proves itself as a icon of power. Specially if the information is confidential and is of critical utility, the power it wields becomes immense. In order to prevent misuse of this enormous power by unauthorized people, security systems have to be implemented to guard the power-base. Security of the data conventionally is relied on the encryption techniques. But, with growing number of established and successful attacks like cryptanalysis or worst case brute force attacks on encryption based systems, this is high time some improved security system has to be developed.

The method of encryption of data, where the data is available to the targeted user with the availability of the decryption key, is popularly known as Cryptography. Steganography is different from cryptography because of the fact that, Cryptography merely converts the data into unintelligible caricature whereas steganography erases even its hint of its presence. Since the classified data is not discernible to the attacker without the secret key, the data remains to be a secret.

The concept of data hiding was firstly proposed by Simmons in 1983 [2]. The classified data can be shared over the overt channels as steganography embeds the text in a cover image,

such that the cover image and the stego image is intangible. The targeted user, unless she has the key to retrieve the information cannot retrieve the information. Steganalysis [3] is the method used to detect, identify, and/or extract hidden information. Steganography and cryptography are codependent, each cannot sustain independently.

Steganography can also be achieved by embedding secret data in an unsuspecting medium like image, video or audio, in such a way that the human-perceived quality of the unsuspecting medium is not altered. So, when that medium is transmitted via a channel, mugger cannot ferret out the classified information. Thus, in case of image steganography [4, 5, 6, 7, 8] if the secret data could be encrypted first and then embedded into a cover image, the directive may be successful. The image into which the encrypted data is embedded is called stego-image. The stego-image is meaningful and the distortion between the original image and the stego-image is very small that the human eye cannot distinguish the difference. Due to the stego-image being meaningful, a malicious attacker cannot consciously know the existence of secret data. Based on the view of the security, the scheme of data hiding is more secure than that of data encryption. In general, the techniques of data hiding have to satisfy the following requirements [3, 7, 8].

- *Imperceptibility*: it is an important quality of image steganography that could prevent the attackers from detecting the secrets existing in the stego-image. The secret is eclipsed into the cover in such a manner that the cover and the stego image are hard to distinguish.
- *Hiding capacity*: the cover image should incapacitate significant number of secret bits.

Besides data hiding, watermarking [3] is another technique that is required to hide data into an image. Watermarking has been commonly used to safeguard the copyright of digital images. It embeds a trademark of the owner into the protected image. The owner can prove the ownership of the suspected image by retrieving the embedded trademark. Generally, watermarking has certain characteristic qualities namely

- *Robustness* [3]: Watermark can resist intentional attacks or common image processing attacks such as

sharpening, blurring or rotating. Watermarks are impregnable therefore can be retrieved easily even after it is modified.

- *Imperceptibility* [3]: a watermark should be infixed in an image invisibly. An assailant must not be able to distinguish the watermark from the original image at the same time the quality of watermarked image should not be seriously degraded.
- *Security* [3]: the watermark mark must be made accessible only its proprietor and not anyone else.

From the requirements of data hiding and watermarking, we can find that no matter what the technique of watermarking or data hiding is, they have the similar requirements. Both of the techniques require only that image quality is not hampered due to the embedding and the classified data is correctly extracted either by the proprietor or the targeted end user only. A higher image quality gives people more difficulty to perceive the existence of sensitive or important data for security. There have been several schemes that have been proposed in the yesteryears for data hiding [4, 5, 6, 8]; however

one of the straight solutions of hiding data is to directly replace the Least Significant Bits (LSBs) of each pixel in the cover image with the bits of secret data. Rather than manipulating the MSB of the cover image, these techniques lessen the distortion. However stego image may undergo transmission errors or errors due to faulty compression. If this situation happens, the extracted data from the stego-image will be erroneous. Therefore, we propose a data hiding scheme to meet the terms of One, the quality of the embedding image which should be acceptable that the human eye cannot perceive the embedded data from the stego image and two, the scheme should provide the distortion tolerance so that the legal user can more correctly extract the embedded data from the stego-image. In order to achieve the ability of distortion tolerance, the image quality will be degraded. In order to enable real time transmission and reception on regular data systems like internet to be used in all areas, the security of the data has to be addressed. The data handled in real time can be illegally used, if not protected by appropriate means. This paper proposes a means to implement measures to protect the confidential data handled in real time Systems.

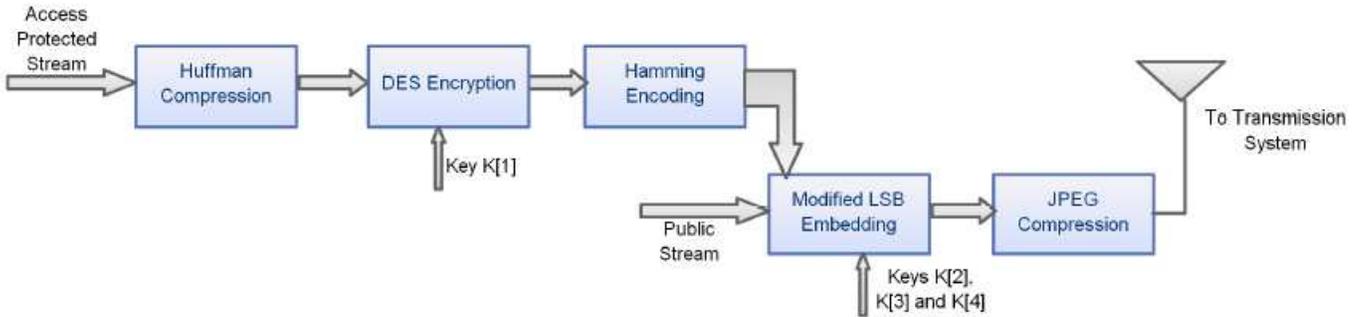


Figure 1. The proposed Embedding system.

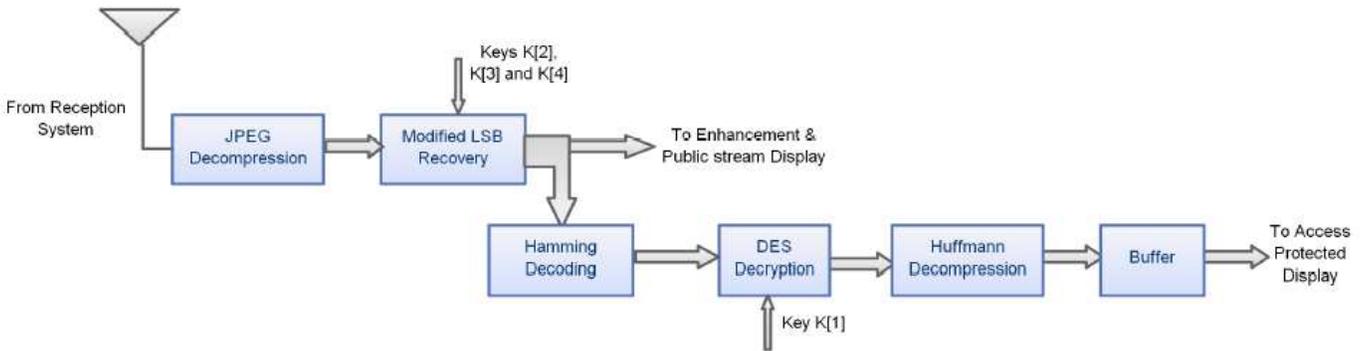


Figure 2. The proposed Extraction system.

II. A NOVEL SECURITY SOLUTION

We take the example of real time system like a Two-Layered Surveillance System as shown in Fig. 1 & 2, which handles two streams of image data, a public stream and an access protected stream. The public stream has no access restrictions. However, the access protected stream has to be interpreted only by authenticated sources. So, it can also be called as secret stream. By use of Steganographic techniques like "Modified LSB Embedding", the data in secret stream can be embedded into the LSB of pixels of public stream. This

embedding is done in an intelligent way, not distorting the public stream, so that any attacker does not visually recognize the reduction in quality of the public stream.

In order to reduce the bandwidth consumption, the secret stream is compressed using a lossless compression technique namely, Huffmann Compression [9]. In order to be resistant against steganalytic attacks, the compressed data is encrypted using DES. In order to impart error correction, the encrypted data is encoded using an error correction code namely, Hamming Code [10]. After embedding the secret stream into

the public stream, it is compressed using JPEG compression and transmitted.

III. IMPLEMENTATION & RESULTS

In this paper, a scaled-down replica of the above-mentioned system is developed, analyzed and the relevant quality metrics are presented. In this scaled-down replica, the following changes in the above method are considered for the sake of ease of analysis only.

- A secret gray-scale image is considered in place of secret stream.
- A public gray-scale image is considered in place of public stream.

A. Transmission

Inputs:

1. Gray-scale public image P and Gray-scale secret image S
2. Key K[1], symmetric key for DES
3. Key K[2], used as seed for randomization
4. Key K[3], number of bits per pixel embedded $K[3] \in \{1,2,3,4\}$
5. Key K[4], for Modified LSB Embedding $K[4] \in \{1,2,4\}$

Output:

1. Gray-scale stego image M

Algorithm:

1. Apply Huffman Compression on S.
2. Let L = number of pixels in P.
3. Encrypt S using DES with key K[1].
4. Encode S with Hamming code.
5. Generate a Pseudo-random sequence R with data in range [1,L] using K[2] as seed.
6. Let index i=0
7. While (i <= L) do the following:
 - 7.1. Embed next K[3] bits of S in P[i] using Modified LSB Embedding (K[4] as key) and store as M[i]
 - 7.2. i = i + 1
8. Apply Optimal Pixel Adjustment Process on resultant image to reduce Mean Square Error.
9. Compress M using JPEG and transmit.

B. Reception

Inputs:

1. Received Gray-scale stego image M
2. Key K[1], symmetric key for DES
3. Key K[2], used as seed for randomization
4. Key K[3], number of bits per pixel embedded $K[3] \in \{1,2,3,4\}$
5. Key K[4], for Modified LSB Recovery $K[4] \in \{1,2,4\}$

Outputs:

1. Gray-scale public image P
2. Gray-scale secret image S

Algorithm:

1. Apply JPEG decompression on M.
2. Let L = number of pixels in M.
3. Generate a Pseudo-random sequence R with data in range [1,L] using K[2] as seed.

4. Let index i=0

5. While (i <= L) do the following:

- 5.1. Restore next K[3] bits of S from M[i] using Modified LSB Recovery (K[4] as key) and store as S[i]

- 5.2. i = i + 1

6. Enhance M and process/store it as public image.

7. Decode S using Hamming Decoding.

8. Decrypt S using DES Decryption with key as K[1].

9. Decompress S using Huffman Decompression.

10. Store it in a buffer and process/store it as secret image.

C. Analysis of various cases

Let us consider an example where the Pixel value is 160 and the secret Binary value= 1001.

Case-1: Without Optimal Pixel Adjustment Process the stego pixel value= 169(10101001) whereas with OPAP the modified Stego- Pixel value= 153(10011001). In the Extraction phase, $\text{MOD}(S,2^k)$ is calculated, where S= stego pixel value, K=no. of bits (here 4).

Case-2: In case of the embedding of 001 from k=2 position, the Pixel value= 160, Message bit= 001. After embedding the data without OPAP, the Stego pixel value=162(10100010) whereas with OPAP the modified Stego pixel value= 162(10100010). The extraction with and without OPAP using $\text{MOD}(S,2^k)$ will give last 4 bits (0010). So, the last bit is discarded to get the message bits.

Case-3: In the case of embedding 2 bits in k=3, 4 position with Pixel value= 160(10100000), Message bits =11. During the embedding phase without OPAP, the Stego pixel value= 172(10101100). With OPAP, the modified Stego pixel value= 156 (10011100), Extraction will be carried out with $\text{MOD}(S,2^k)$. The extraction process gives 1100 so, the last 2 bits are discarded to get the message bits.

Case-4: In case of embedding 1 bit only in 4th position the Pixel value=160 with Message bit= 1, during the Embedding phase, without OPAP, the Stego pixel value=168 and with OPAP, the modified Pixel value= 168. Extraction, carried out using $\text{MOD}(S,2^k)$, gives 1000 so, the last 3 bits are discarded to get the message bits.

D. Error Metrics

Distortion in the stego image is measured by means of four parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), number of errors and Bit error rate.

- MSE is calculated by using the equation,

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (X_{i,j} - Y_{i,j})^2 \quad (1)$$

where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image X_i, j represents the pixels in the original image and Y_i, j , represents the pixels of the stego-image.

- Peak Signal to Noise Ratio (PSNR) is calculated using the equation,

$$PSNR = 10 \log_{10} \left(\frac{I_{\max}^2}{MSE} \right) dB \quad (2)$$

where I_{\max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the value of PSNR better the image quality.

• Bit Error Rate (BER) and Bit Error

BER evaluates the actual number of bit positions which are replaced in the stego image in comparison with cover image. It has to be computed to estimate exactly how many bits of the original cover image (I_c) are being affected by stego process. The BER for the Stego image (I_s) is the percentage of bits that have errors relative to the total number of bits considered in I_c . Let I_{cbin} and I_{sbin} are the binary representations of the cover image and stego cover then,

$$T_e = \sum_{i=1}^n |I_{cbin} - I_{sbin}|$$

$$\text{and the bit error rate BER} = \frac{T_e}{T_n}$$

T_n is the total number of bits considered for the gray image of size $M \times N$ pixels, T_n will be $M \times N \times 8$.

IV. RESULT & DISCUSSION

In this present implementation Lena and baboon of 256×256 digital images have been considered as cover images as shown in Fig. 3, 4 a & b and tested for full embedding capacity for $k=2$ embedded in 2 bit position given in Fig. 2 a & b and with varying positions {1, 2, 3, 4} and k values for {1, 2, 3, 4} the MSE, PSNR and Bit error rate given in Fig. 5 a, b & c.

The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for the two digital images. The result data shows that for ordinary LSB embedding with k (number of LSBs used) = 4, the Mean Square Error is less. But, as the 1st LSB is used here, it is not resistant to data loss during JPEG compression or Zip compression.

In case of modified LSB embedding with $k=2$ and 3, since the embedding is performed leaving the 1st LSB, embedding capacity is lesser than that for ordinary LSB embedding. But, this is resistant to JPEG compression losses in stego image, leading to a lesser bit error rate after recovery.

The reduction in embedding capacity is compensated by Huffman compression, which compresses the data before embedding. Distortion, if any, due to external sources or compression, gets automatically corrected since Hamming encoding (an error-correcting code) is employed. The usage of DES adds still more security to the data against steganalytic attacks.

Since this method transmits, two streams of data in a single image, effective channel utilization becomes less thus, leading to bandwidth saving. The distortions introduced due to embedding in the public stream, can be corrected to restore the visually perceived quality by appropriate enhancement and other image processing techniques.

Thus, the use of this methodology gives a combo of advantages namely,

- unsuspecting security
- Bandwidth efficiency
- Effective separation of confidential and casual information

The experiment presented in this paper could be extended to suit this methodology to all sorts of data namely, textual, audio, video, etc. without any major changes in the methodology.

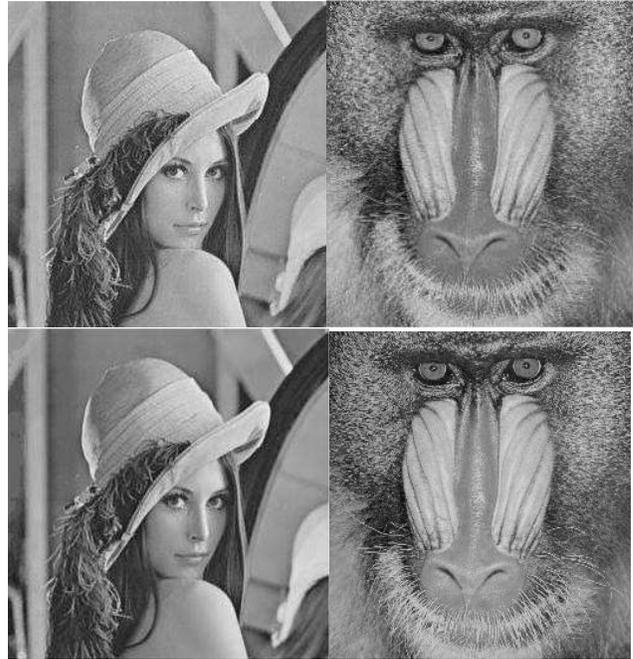


Figure 3 a & b Cover & Stego for Lena Image

Figure 4 a & b Cover & Stego for Baboon Image

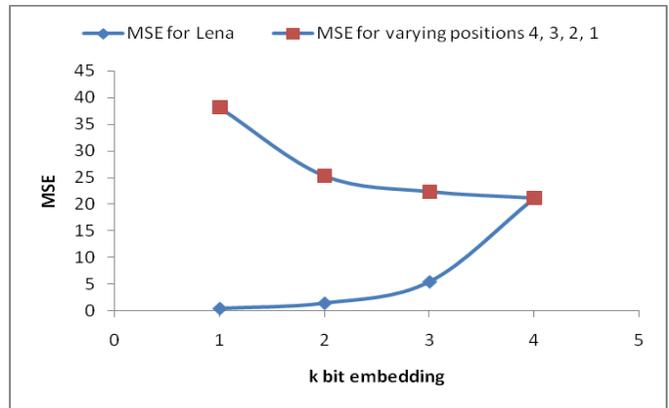


Figure 5 a MSE for K= 1, 2, 3 and 4 for varying bit position 4, 3, 2 and 1.

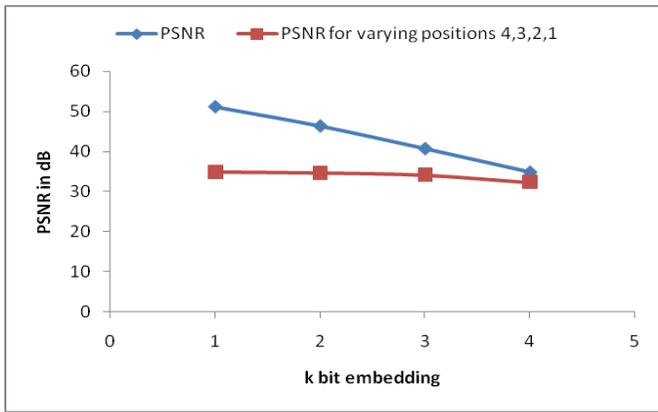


Figure 5 a PSNR f for K= 1, 2, 3 and 4 for varying bit position 4, 3, 2 and 1.

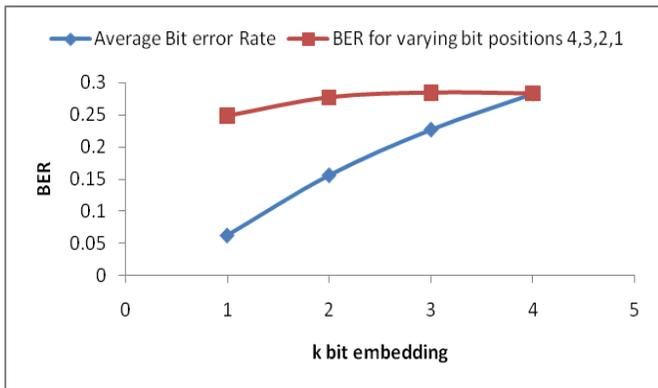


Figure 5 c BER for K= 1, 2, 3 and 4 for varying bit position 4, 3, 2 and 1.

V. CONCLUSION

In the proposed method, the usage of Hamming encoding protects the data against distortion. Lossless Huffman compression increases the effective embedding capacity offered by the technique as a whole. Increased security, provided by the encryption makes this technique resistant to steganalytic attacks. Modified LSB embedding performs the vital job of hiding the secret data in a recoverable and secure manner. Since the proposed 'twin-stream steganography based security' uses all these, it proves itself to be a self sufficient security solution for real time environment. In the present work steganalysis is not taken into consideration. How the system withstands distortion during compression will be considered as a future work. The present work has taken the gray image as public data stream (as cover image), if implemented in colour image then capacity of the system will improve. Furthermore it will improve the complexity of the proposed system.

ACKNOWLEDGMENT

The authors wish to thank G Aishwarya, S Mohammed Shakeel, Motamarri Abhilash swarup, Mohamed Ashfaq K, and Sandeep Kumar Behera Stego group Students Department of Electronics & Communication / SEEE for their technical support.

REFERENCES

- [1] Bruce Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007.
- [2] G. J. Simmons, "The prisoners' problem and the subliminal channel," in Proc. IEEE Workshop Communications Security CRYPTO'83, Santa Barbara, CA, 1983, pp. 51-67.
- [3] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
- [4] R.Amirtharajan, R. Akila, P.Deepikachowdavarapu, "A Comparative Analysis of Image Steganography". International Journal of Computer Applications 2(3):(2010)41-47.
- [5] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods Signal Processing 90 (2010) 727-752.
- [6] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313-336.
- [7] Peter Wayner, "Disappearing cryptography: information hiding : steganography & watermarking" 2nd. ed. San Francisco: Morgan Kaufmann; 2002.
- [8] R.Amirtharajan, Krishnendra Nathella and J Harish, "Info Hide - A Cluster Cover Approach" International Journal of Computer Applications 3(5)(2010) 11-18
- [9] Behrouz Forouzan, "Data Communications and Networking" 2nd. ed. McGraw-Hill, 2001.
- [10] Thomas L. Floyd, "Digital Fundamentals" 9th Edition Pearson Prentice Hall, 2009.

AUTHORS PROFILE

R. Amirtharajan was born in Thanjavur, Tamil Nadu province India, in 1975. He received B.E. degree in Electronics and Communication Engineering from P.S.G. College of Technology, Bharathiyar University, Coimbatore, India in 1997 and M.Tech. in Computer Science Engineering from SASTRA University Thanjavur, India in 2007. He joined SASTRA University, Thanjavur, Tamil Nadu, India (Previously Shanmugha College of Engineering) as a Lecturer in the Department of Electronics and Communication Engineering since 1997 and is now Assistant Professor. He is currently working towards his Ph.D. Degree in SASTRA University. His research interests include Image Processing, Information Hiding, Computer Communication and Network Security. So far he filed one International Patent; he has published 10 Research articles in National & International journals. He has Supervised 10 Master Students and more than 100 UG projects. Currently he is working on funded project in the field of Steganography supported by DRDO, Government of India, New Delhi.

Vivek Ganesan and Jithamanyu are former Stego group B.Tech. Students of the Department of Electronics and Communication Engineering, School of Electrical & Electronics Engineering, SASTRA University. Apart from excellent academic record, they presented 3 papers in various National Level Student Symposiums. They also won the coveted first prize in Hardware Design Competition held at SEEE, SASTRA University. They qualified as finalists in The Great Mind Challenge, an application development contest conducted by IBM in the year 2008. They also won the honorable first prize in the Web Design Contest conducted by Microsoft at SRM University and appointed as Microsoft Student Ambassadors of SASTRA University.

John Bosco Balaguru Rayappan was born in Trichy, Tamil Nadu province, India in 1974. He received the B.Sc., M.Sc. and M.Phil. Degree in Physics from St. Joseph College, Bharathidasan University, Trichy and Ph.D. in Physics from Bharathidasan University, Trichy, Tamil Nadu India in 1994, 1996, 1998 and 2003, respectively. He joined the faculty of SASTRA University, Thanjavur, India in Dec 2003 and is now working as Professor in School of Electrical and Electronics Engineering at SASTRA University, Thanjavur, Tamil Nadu, India. His research interests include Lattice Dynamics, Nanosensors, Embedded System and Steganography. So far he has published 22 Research articles in National and International journals and 14 conference papers. He has Supervised 25 Master Students and Supervising 3 Ph.D. Scholars. Currently he is working on four funded projects in the fields of Nanosensors and Steganography supported by DST and DRDO, Government of India, New Delhi.