A New Approach of Image Security through Combination of Steganography and Cryptography

[1]Pawan Singh Rajput, [2]Smt. Sunita Gond
[1]BU IT Bhopal, [2]Prof. BU IT, Bhopal,
Email: pawansingh_r@yahoo.com, sun11g@yahoo.com

Abstract: **Steganography is a technique to make secret message imperceptible to human eyes by embedding it in some vessel data/information/images (multimedia Data). We call another multimedia data like an image part of the vessel data external information (cover image), and the embedded data internal information (secret image). The internal information (secret image) is not so valuable to the data owner itself. Digital Steganography exploits the use of a host data to hide a piece of information in such a way it is imperceptible to a human observer. In this paper an image Steganography system, in which the data hiding (embedding) is realized in bit planes of encrypted image by using cryptography technique is implemented. To increase data hiding capacity while keeping the imperceptibility of the hidden data, cryptography technique has. The proposed system shows a high data hiding capacity. All of the traditional steganography techniques have limited information-hiding capacity. They can hide only 10% (or less) of the data amounts of the vessel. Our new Steganography system uses, an image as the vessel data,, and we embed secret information/image in the bit-planes of the image by using standard steganography technique (LSB Technique). Presented results are proving/showing the performance of the proposed system.**

Keyword: **Security, Image, Network, Algorithm, Key**

I. INTRODUCTION

The primary tool used in the research of steganography and cryptography is the Internet. The first thing was to understand the various terminologies related to the field. This was done through the previous research papers, books and the hyper dictionary websites. Additional technical details were obtained from various articles listed under the references section [1, 2]. The following points can be attributed to the renaissance of steganography: Government ban on digital cryptography, for Individuals as well as companies who seek secrete/confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy. The increased need to protect intellectual property rights by digital content owners, using efficient watermarking. The trend towards electronic communications and humans desire to conceal messages from curious eyes [3, 4]. With rapid growth/advancement in technology/technique, steganography software is becoming effective in hiding information in image, audio or text files. In this research, a **"**Novel Steganography Approach using Cryptography" is presented by analyzing the principle of the steganography approach based on the combination of steganography and cryptography (symmetric) [5]. Furthermore the Performance and the security of the proposed approach are also evaluated. The Presented results based on the combination of steganography and cryptography (Symmetric) approving the effectiveness of the proposed approach, and the combination of steganography and cryptography show high-level security and provide variation in key space [6]. The produced cipher image through this method may be approximately same in size as the original image and suitable for the secure transmission of confidential image over the Internet.

Rest of the Paper is organized as follow: Section II is the proposed work in this proposed concept about image encryption and steganography is presented; Section III is the results analysis. In this results performance of proposed image encryption algorithm are presented finally Section IV is the conclusion. In this overall conclusion of the paper are presented.

II. PROPOSED WORK

2.1 Proposed Concept: Multimedia Information provides a robust and easy modification/editing in information. The Information can be transmitted over public networks without any error and often without interference. But unfortunately, digital media distribution raises a concern for digital content owners. Digital information could be copied without any loss in content and quality. This poses a big problem to the protection of intellectual property rights. Watermarking technique is the solution to the problem. This can be defined as embedding digital information/data, such as information about the owner/sender, recipient/receiver, and access level, without being findable/detectable in the host multimedia data [11-13]. Proposed work entitled "Design and Implementation of a Novel Steganography Approach using Cryptography" is proposed by analyzing the principle of the image steganography technique with cryptography (Symmetric) [14]. Proposed approach support to basic security principal like integrity, authorization, and accuracy of confidential images in the network. It's known that, lots of effort is required during steganography with image encryption/decryption. Proposed approach introduces a new symmetric encryption algorithm. With the secrete image read the binary value and divided into two equal parts, where binary value of each part of secrete image mapping with each other. After completing mapping process read binary value from new mapped images, these binary

values again mapped with symmetric encryption approach in proper way to produced encrypted images which is called cipher image. The Proposed image encryption/decryption used a key value during encryption/decryption process. This key value is providing higher security for the proposed approach. Strength of the proposed symmetric encryption/decryption algorithm is that its take a block of 128 bits or 16 byte at a time for encryption/decryption which is highly secured and is suitable for practical use in the secure transmission of secured information over the public network. Furthermore produced cipher image embedded with cover image through standard steganography approach. Generated stego-image same in size as compare cover image after steganography process. The receiver ends the stego-image, decrypts it to obtain the encrypted image and analyses this stego-image with the cover image to reconstruct the cipher image. This cipher image is once again decrypted to obtain the secret image. Figure 1 showing the block diagram of the proposed technique at encryption and decryption end respectively

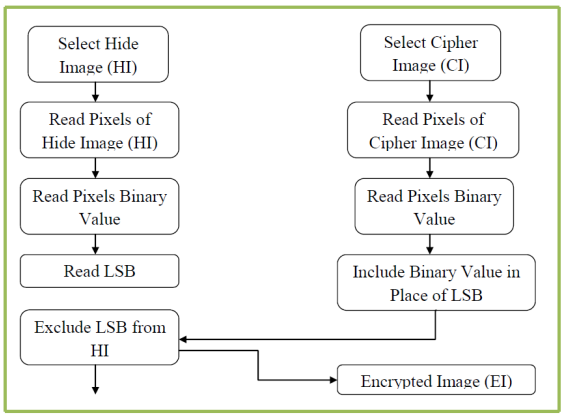


Figure 2.1 : Block Diagram of Proposed Steganography at Encryption/Decryption Side

2.2 Steganography Algorithm Steps:- steganography algorithm steps at sender end is in section 2.2.1 and steganography algorithm step at receiving end is in section 2.2.2.

2.2.1 Steganography Algorithm Steps at Sender Side:-

Input a Encrypted Image (EI) and Cover Image (CI).
Read Binary of EI and CI.
Extract Least Significant Bit (LSB) from Cover (CI)
Swap LSB of CI with Binary Value of EI
Produced Stego-Image (SI)

2.2.2 Reverse Steganography Algorithm Steps at Sender Side:-

Select Encrypted Image (EI).
Read Least Significant Bit (LSB) from EI.
Collect all LSB value from EI.
Prepare Cipher Image (CI) from LSB value.
Distinguish Hide Image (HI) and Cipher Image (CI) from Encrypted Image (EI)

2.3 Proposed Encryption Approach: In this binary value of hided image (HI) are mappings or XORed with key value (K) where key value to produce encrypted value (EV). Then Read 16 bytes or 128 bits value from encrypted value at a time and shift K^{th} (SK^{th}) time (16^{th} time in left), this produced shifted value (SV). This process will continue for every 16 byte or 128 bit encrypted value till last of the encrypted value and converted it into corresponding color pixels (CP). After this an encrypted image (EI) created and read red, green and blue (RGB) value from this and mapped or XORed with read red, green and blue (RGB) value of covered image (CI) to produce final encrypted image. Architecture of the proposed encryption process is shown in figure 2.2.

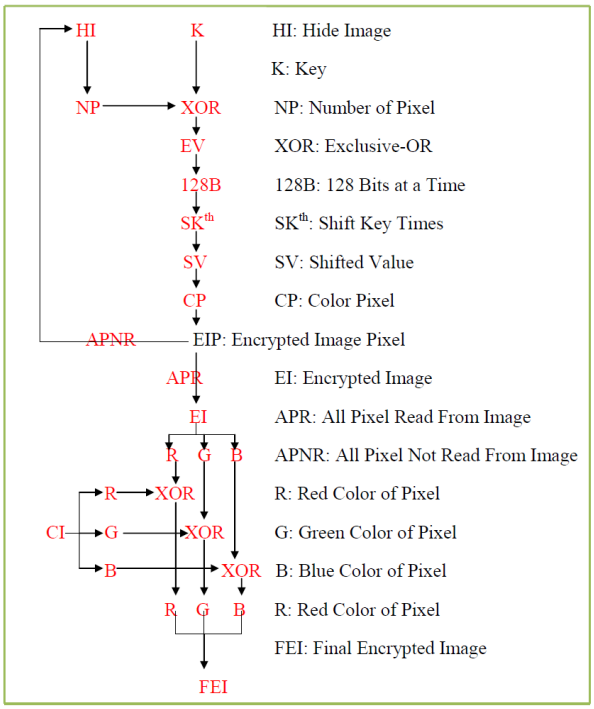


Figure 2.2: Architecture of Proposed Encryption

2.4 Proposed Decryption Approach: Decryption is just reverse process of encryption. In this red, green and blue (RGB) pixel value of final encrypted image (FEI) are mappings or XORed with red, green and blue (RGB) pixel value of cover image (CI) to produced encrypted image (EI) key value where key value to produce encrypted value (EV). Then Read 16 bytes or 128 bits value from encrypted value at a time and reverse shift K^{th} (RSK^{th}) time (16^{th} time), this produced shifted value (SV). This process will continue for every 16 byte or 128 bit encrypted value till last of the encrypted value. After this shifted value (SV) mapped or XORed with key value (K) to produce original image pixel

(OIP). Architecture of the proposed encryption process is shown in figure 2.3.

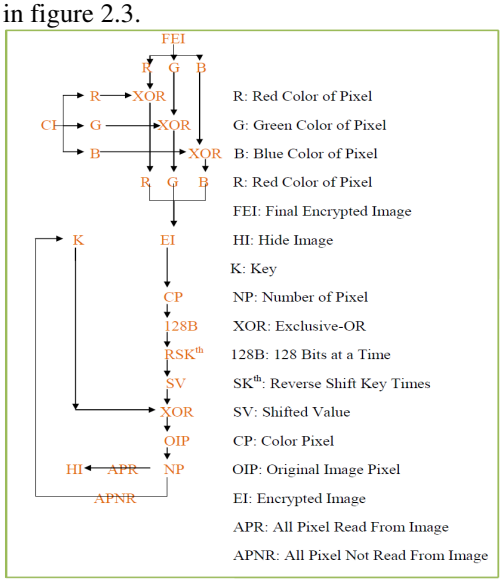


Figure 2.3: Architecture of Proposed Decryption

2.5 Algorithm Step: Proposed encryption algorithm Step are defining in section 2.5.1 and proposed decryption algorithm step are defining in section 2.5.2.

2.5.1 Algorithm Of Proposed Encryption

Input Hide/Confidential Image (HI)
Input Key value of 16 Bytes long
Input Cover Image (CI)
Read total pixel value from HI.
Perform Exclusive-OR (XOR) operation Between K and Pixel of (HI) to produced Encrypted Image (EI)
Read 128 bits at time from EI.
Shift (left) to 128 bits, k^{th} (16) times.
Repeat 6^{th} and 7^{th} Step to all bits of EI.
Read RGB Color value from CI and EI.
Perform Exclusive-OR (XOR) operation between RGB of CI and RGB of EI individually to produce Final Encrypted Image (FEI)
Exit.

2.5.2 Algorithm of Proposed Decryption

Input Final Encrypted Image (FEI)
Input Key value of 16 Bytes long
Input Cover Image (CI)
Read RGB Color value from CI and FEI
Perform Exclusive-OR (XOR) operation between RGB of CI and RGB of FEI individually to produce Encrypted Image (EI)
Read total pixel value from FEI.
Read 128 bits at time from EI
Shift (left) to 128 bits, k^{th} (16) times in reverse order.
Repeat 7^{th} and 8^{th} Step to all bits of EI.
Perform Exclusive-OR (XOR) operation Between K and Pixel of (EI) to produced Hide/Confidential Image (EI)
Exit.

2.6 Proposed Paradox at One End: Paradox at One end is shown in figure 2.4 where steganography and cryptograph are executing with each other but in proper way. First cryptography followed by steganography approach executed. In this two images (Hided, Cover) pass as an input where hided image work with proposed encryption/decryption and cover image work with steganography approach.

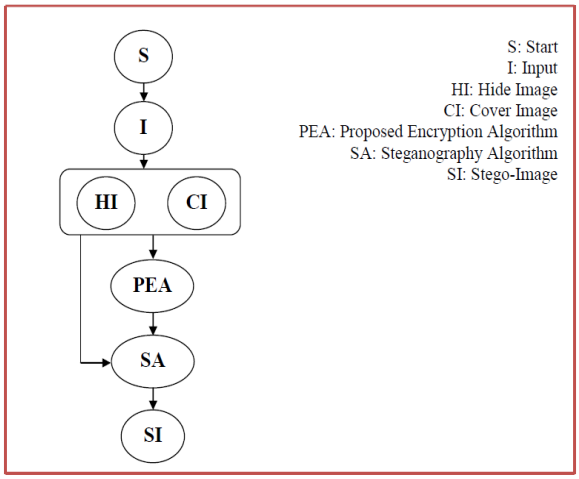


Figure 2.4: Block Diagram of Proposed Paradox in One End

2.7 Proposed Reverse Paradox at another End: Paradox at another end is shown in figure 2.5 where reverse steganography and reverse cryptograph are executing with each other but in proper way. First reverse steganography followed by cryptography approach executed. In this two images (stego, Cover) pass as an input stego-image work with reverse steganography approach and produced cipher image from stego-image work with proposed encryption/decryption

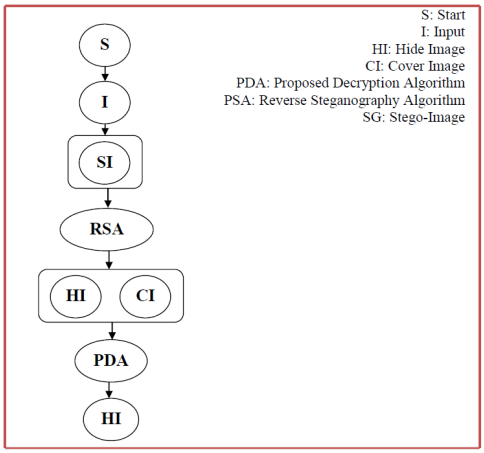
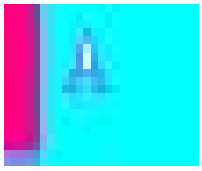


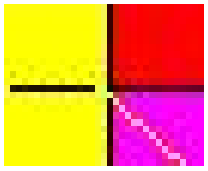
Figure 2.5: Block Diagram of Proposed Reverse Paradox at another End

III. RESULTS

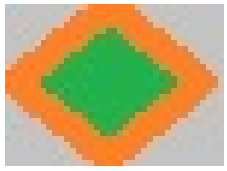
3.1 During results calculation various size of image encrypted/decrypted and generated final stego image and approximately 100 times run to the proposed system, after that noted down performance parameters (PSNR, Entropy and Histogram) [7, 8, 9] which is shown in table 5.1 to 5.3. In every time, same size of images are respectively encrypted/decrypted and generated stego image by existing and proposed algorithm by copying them. Size of the selected key was same in each time. Finally, the outputs of the comparison system are entropy and correlation which is noted in numeric form. For Results Evolution I have selected four Input images and four Cover image which is shown below.



Input Image 1



Input Image 2



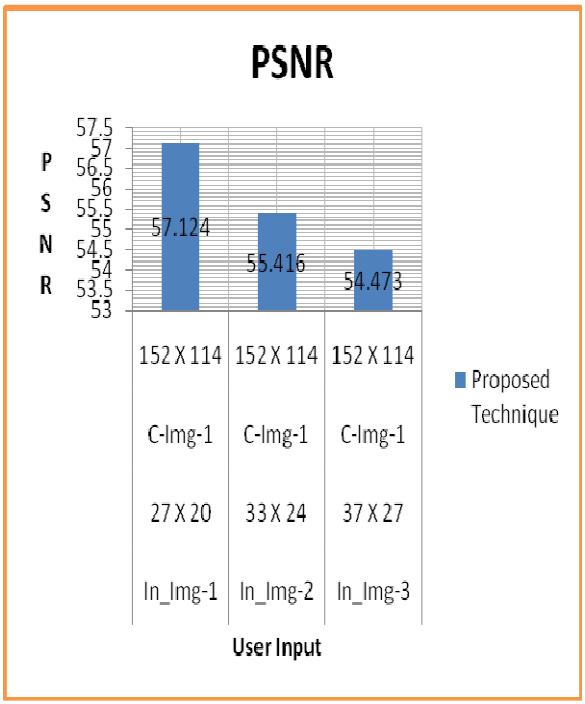
Input Image 3

Cover Image 1

3.1.1 Peek Signal to Noise Ration (PSNR): - "The Proposed Technique" have been implemented on a number of image varying types of content and sizes of a wide range. PSNR of Various images comparisons shown in table 3.1 & graph 3.1

Table 3.1: PSNR Analysis of Stego Images through Proposed

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Technique
	Approx Stego Image PSNR				
1	In_Img-1	27 X 20	C-Img-1	152 X 114	57.124
2	In_Img-2	33 X 24	C-Img-1	152 X 114	55.416
3	In_Img-3	37 X 27	C-Img-1	152 X 114	54.473



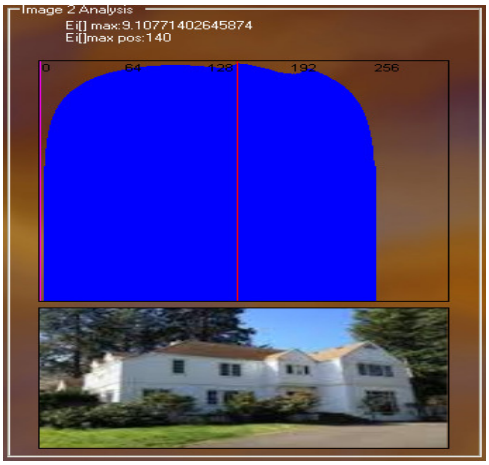
Graph 3.1: PSNR Analysis of Stego Images through Proposed Technique

3.1.2 Stego Image Entropy: "The Proposed Technique" have been implemented on a number of images varying types of content and sizes of a wide range. Encrypted image entropy of various images comparisons shown in table 3.2.

Table 3.2: Entropy Analysis of Stego Images through Proposed Technique

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Techique
	Stego Image Entropy (Approx)				
1	In_Img-1	27 X 20	C-Img-1	152 X 114	9.11014
2	In_Img-2	33 X 24	C-Img-1	152 X 114	9.10787
3	In_Img-3	37 X 27	C-Img-1	152 X 114	9.11189

Graph 3.2: Entropy Analysis of Stego Images through Proposed Technique of Input Image 1



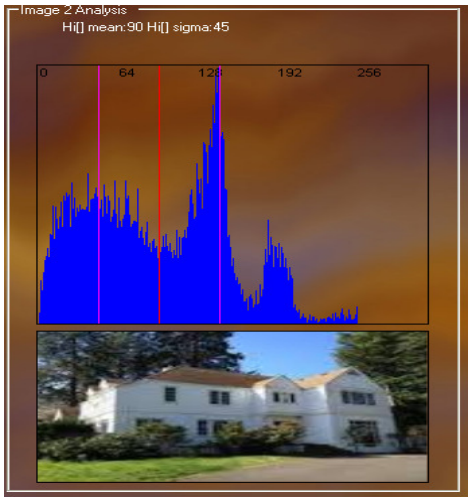
Graph 3.3: Entropy Analysis of Stego Images through Proposed Technique of Input Image 2

Graph 3.4: Entropy Analysis of Stego Images through Proposed Technique and Existing Technique of Input Image 3

3.1.3 Histogram: - "The Proposed Technique" have been implemented on a number of image varying types of content and sizes of a wide range. Histogram of Various images comparisons shown in table 3.3.

Table 3.3: Histogram Analysis of Stego Images through Proposed Technique

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Technique	
	Stego Image Histogram (Approx)					
					Mean	Sigma
1	In_Img-1	27 X 20	C-Img-1	152 X 114	90	45
2	In_Img-2	33 X 24	C-Img-1	152 X 114	90	45
3	In_Img-3	37 X 27	C-Img-1	152 X 114	90	45



Graph 3.5: Histogram Analysis of Stego Images through Proposed Technique of Input Images

3.2 Results Analysis: From table 3.2 its observed that entropy of stego image are evaluating through maximum entropy value of encrypted pixel, in two case proposed algorithm producing higher value in terms of entropy and in but in some cases proposed technique cannot be produced good results but in general maximum time our proposed technique are producing good results in terms of entropy. For example input image-1 producing 9.110 entropy value through proposed algorithm and For example input image-2

producing 9.107 entropy value through proposed algorithm For example input image-3 producing 9.11189 entropy value through proposed algorithm. From table 3.3 it's observed that histogram of stego image are evaluating through two parameters one is mean value (mean) of encrypted pixel and another is sigma value of encrypted pixel, in all three case proposed algorithm are producing same histogram value. For example input image-1, 2, 3 producing 90 mean value and 45 sigma value through proposed algorithm. The most important parameter of the proposed research is peek signal to noise ratio (PSNR) which is show in table 3.1 for various images. Through numeric value of table 3.1 to 3.3 and graph 3.1 to 3.4 it's easy analyzed that stego image of picture quality of proposed algorithm is batter then previous algorithm.

IV. CONCLUSION

Proposed Standard Steganography technique is not intended to replace cryptography but rather to supplement it. A message is encrypted and hidden with a suggested standard steganography method it provides an additional layer of protection and reduces the chance of the hidden message being detected. Steganography is still a fairly new concept to the general public although this is likely not true in the world of secrecy and espionage. Efforts to improve the robustness of the proposed technique are necessary to ensure that the steganography and cryptography technique can securely defend against any type of attacks. With continuous advancements in technology it is expected that in the near future more efficient and advanced techniques in steganalysis will emerge that will help law enforcement to better detect illicit materials transmitted through the Internet. The proposed work introduces a part of the art of steganography.

REFERENCES

[1] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM - 2012) March 30, 31, 2012

[2] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012.

[3] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[4] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[5] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012

[6] AmrM. Riad, Amr H. Hussein and AtefAbou EI-Azm "A New Selective Image Encryption Approach using Hybrid Chaos and Block Cipher "The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Computational Intelligence and Multimedia Computing Track

[7] Arun Raj R, Sudhish N George and Deepthi P. P. "An Expeditious Chaos Based Digital Image Encryption Algorithm" 1st Int'l Conf. on Recent Advances in Information Technology | RAIT-2012 |

[8] Rithmi Mitter and M. Sridevi Sathya Priya "a highly secure cryptosystem for image encryption" IEEE Conferences 2012

[9] Somdip Dey, Kalyan Mondal, Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm" I.J.Modern Education and Computer Science, 2012, 6, 59-67 Published Online June 2012 in MECS (http://www.mecs press.org/)DOI: 10.5815/ijmecs.2012.06.08

[10] S.Premkumar, A.E.Narayanan "Steganography Scheme Using More Surrounding Pixels combined with Visual Cryptography for Secure Application "International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

[11] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

[12] danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

[13] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[14] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE