

Security Improvisation in Steganography using AES 128/192/256

Deshmukh Priyanka Pravin
PG Student,

Department of Computer Science and Engineering,
JNEC, Aurangabad, India.

Smita Kasar

Assistant Professor,
Department of Computer Science and Engineering,
JNEC, Aurangabad, India.

Abstract— We live in the world of Internet, the “Age of Information Technology” where a large amount of private and confidential information is being stored, processed and transmitted. Such data has become susceptible to copyright infringement, eavesdropping, and hacking, cracking and other kind of unauthorized access. So it is necessary to maintain the confidentiality and the integrity of this data. This has given rise to the need of secret communication. As a result a new domain dealing with security of data has evolved and is known as “Information Hiding”. Our system makes the combined use of the two data hiding techniques i.e., Cryptography and Steganography that allows the user to compress the Secret-Image using Zipped compression followed by AES 128/192/256 encryption and hiding the same into other Cover-Image thus providing high level of secrecy and security.

Keywords: Cover-Image, Secret-Image, Stego-Image, AES.

I. INTRODUCTION

We live in the world of Internet, the “Age of Information Technology” where a large amount of private and confidential information is being stored, processed and transmitted. E.g.: Credit card numbers, bank statements, patient medical records and history, etc. Such data has become susceptible to copyright infringement, eavesdropping, and hacking, cracking and other kind of unauthorized access. So it is necessary to maintain the confidentiality and the integrity of the data. This has given rise to the need of secret communication. As a result a new domain dealing with security of data has evolved and is known as “Information Hiding” which covers applications such as copyright protection for digital media, Cryptography, Steganography, Digital Watermarking and fingerprinting [1]. Cryptography and Steganography are considered to be among the top ten information hiding techniques.

According to the definition of Oxford English Dictionary, Cryptography can be defined as: “A secret manner of Writing...Generally, the Art of Writing or Solving Ciphers...”

The word “Cryptography” is derived from the Greek word “Cryptos” which means “Hidden” and “Grapia” which means writing or drawing [2]. Thus Cryptography stands for “Hidden Writing”. Cryptographic techniques “scramble” messages (plain text into cipher text) so if intercepted, the

messages cannot be understood. Plain text can be simply text, an image, an audio or a video. Cipher text is the unreadable or unintelligible data. The process of conversion of plain text to cipher text is called encryption while the process of conversion of cipher text to plain text is called decryption.

Cryptographic technique changes the message so that it cannot be understood but this can generate curiosity level of an intruder. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden or not. The idea results in Steganography, a branch of information hiding by hiding secret information within other information.

According to the definition of Oxford English Dictionary, Steganography can be defined as: “The practice of Concealing Messages or Information within other Non-Secret Text or Data...”

The word “Steganography” is derived from Greek “Steganos” meaning covered or concealed or secret and “Grapia” which means writing or drawing. Thus, “Steganography” stands for “Covered Writing” [3]. Steganography in the modern day usually refers to information or a file that has been concealed inside a digital Picture or an Audio or a Video or another file.

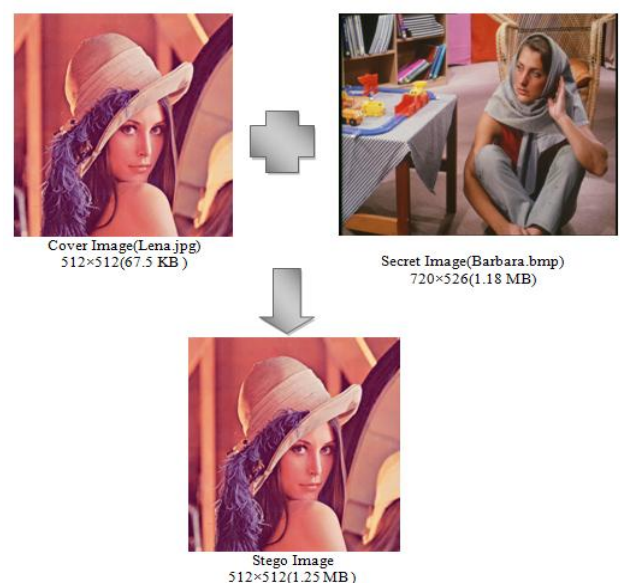


Figure 1: The Block Diagram of Steganographic System

Steganography is all about creating a form of secret communication between two parties and it is a complement of

Cryptography whose goal is to conceal the content of a message. Steganography uses a medium like an image, video, audio or text file to hide some information inside it in such a way that it does not attract any attention and looks like an innocent medium [4]. The media with and without hidden information are called Stego-media and cover-media, respectively [5].

Cryptography and Steganography are widely used in the field of data hiding and have received significant attention from both industry and academia in the recent past. Former conceals the original data but latter conceals the very fact that data is hidden. Steganography provides high level of secrecy and security by combining with cryptography. Steganography with cryptography provide powerful tools for image security over communication. There are various cryptographic technique combined with Steganography for additional security [6, 7].

II. RELEVANT TERMINOLOGIES

All Steganography systems, irrespective of the algorithms by which they are implemented adhere to the following terms [1].

(i) **Message/ Data-File/Secret- Media:** The Message/Data file/ Secret- Media is the secret information which needs to be protected against copyright infringement, eavesdropping, and hacking, cracking and other kind of unauthorized access by making it invisible or hidden. It can be a simply text, text file, an image, an audio, video, etc.

(ii) **Cover- Media:** The cover media is the carrier of the hidden secret information. A cover is generally chosen in a manner that it appears most ordinary and innocuous and does not arouse suspicion as such. A cover medium can be a text file, HTML file, an image, an audio, a video, etc.

(iii) **Stego-Medium:** The cover medium with a secret information (message/Data-File/Secret-Medium) concealed within it is known as the *Stego* medium.

Stego-Medium=Cover-Media + Message/Data-file/Secret-Medium

(iv) **Stego-Key:** Stego key is a key to embed data in a cover and extract data from the Stego medium.

(v) **Embedding Domain:** The Embedding domain refers to the cover-medium characteristics that are exploited in embedding message into it. It may be spatial domain when direct modification of the constituent elements of the cover is modified (e.g. pixels in an image) or it can be the frequency domain or transform domain if mathematical transformations are carried on the medium before embedding.

III. RELATED RESEARCH WORK

There are large numbers of steganography embedding techniques proposed in the literature. These techniques modify the cover image with different methods. But the entire embedding techniques share the substantial goal of maximizing the capacity of the stego channel [6, 7, 8]. In other words, the aim is to embed at highest possible rate while remaining undetectable to Steganalysis attack. Special domain embedding technique operates on the principal of tuning the parameter of the cover image (payload or disturbance) so that the difference between the Cover-Image and the Stego-Image is little and imperceptible to the human eyes.

Steganography generally exploit human perception because human senses are not skilled to look for file that has hidden information inside them. Therefore steganography disguises information from people trying to hack them. Payload is the amount of data that can be hidden in the cover object. The most widely known image steganography algorithm is based on modifying the least significant bit of pixel value, hence known as LSB technique.

A. Peak Signal to Noise Ratio (PSNR) :

The measurement of the quality between the cover image f and stego-image g of sizes $N \times N$ (for 8 bit gray level) is defined by PSNR as:

$$\text{PSNR} = 10 \times \log (255^2 / \text{MSE})$$

$$\text{Where MSE} = \sum_{N=0}^{N-1} \sum_{N=0}^{N-1} (f(x, y) - g(x, y))^2 / N^2$$

Where $f(x,y)$ and $g(x,y)$ represent the pixel value at the position (x, y) in the cover-image and the stego-image respectively. The PSNR is expressed in dB. PSNR is representative of the quality of image i.e. the higher the PSNR, lower in the difference between cover image and Stego image and vice – versa.

B. Steganographic Triangle:

Several important issues need to be considered when studying steganographic systems. They are steganographic robustness, capacity, and security. The affiliation between them can be expressed by the steganography triangle shown in Figure 2. It represents balance of the desired characteristics associated with steganographic method. They are interdependent on each other and in order to improve one element, one or both of other elements needs to be sacrificed.

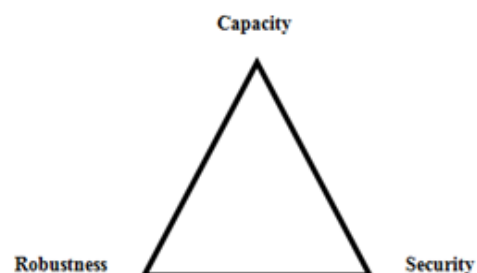


Figure 2: The Steganography Triangle

IV. DESCRIPTION OF AES

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm supports any combination of data and key size of 128/192/256 bits. AES is divided into four basic operational blocks. These operate on array of bytes and organized as a 4×4 matrix called state. For complete encryption, the data is passed through 10 rounds [9].

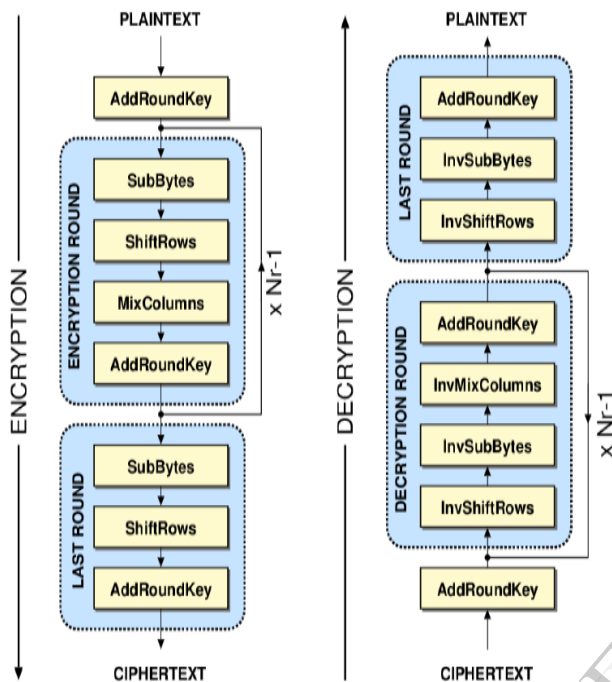


Figure 3: Working of AES Algorithm

Steps:

1) KeyExpansion—Round keys are derived from the cipher key using Rijndael's key schedule.

2) Initial Round

a) AddRoundKey—Each byte of the state (4×4 bytes block) is combined with the round key using bitwise XOR.

3) Rounds(Nr=10,12,14 for 128,192,256 bit keys respectively)

a) SubBytes—A non-linear substitution step where each byte is replaced with another according to a lookup table.

b) ShiftRows—A transposition step where each row of the state is shifted cyclically a certain number of steps.

c) MixColumns—A mixing operation which operates on the columns of the state, combining the four bytes in each column.

d) AddRoundKey

4) Final Round (No Mix Columns)

a) SubBytes

b) ShiftRows

c) AddRoundKey

V. DEVELOPED IMAGE STEGANOGRAPHY MODEL

The proposed system is a secure Steganography System that allows the user to embed or hide **Secret Image** into other **Cover-Image** without affecting the quality of the original **Secret-Image** or the **Cover-Image**. It achieves this by using the least significant bits of these Cover-Images for embedding data which are not used by the Image viewers and Image editors [10][11].

The features of the proposed system are as listed below:

1. Secret Image can be **compressed** by using **ZIP compression** format with the choice of compression level to be used: **low or high**.

2. Secret Image can be **encrypted** by using **128/192/256 bit key AES** encryption algorithm which means that once encrypted, the Secret Image could be retrieved (or decrypted) from a Stego-Image only after specifying the correct password which was used at the time of encryption.

3. Cover-Images supported are: jpg, gif, tiff, bmp, png. Secret Image can be jpg, gif, tiff, bmp, png.

DESCRIPTION:

1. Compression and Encryption Module:

Secret Image is given as an input to the compression module (**Zipped Compression**). Compression level can be set to **low/high**.

The compressed Secret Image is encrypted using **128/192/256 bit key AES** encryption algorithm.

The output of this module is **compressed encrypted** Secret Image.

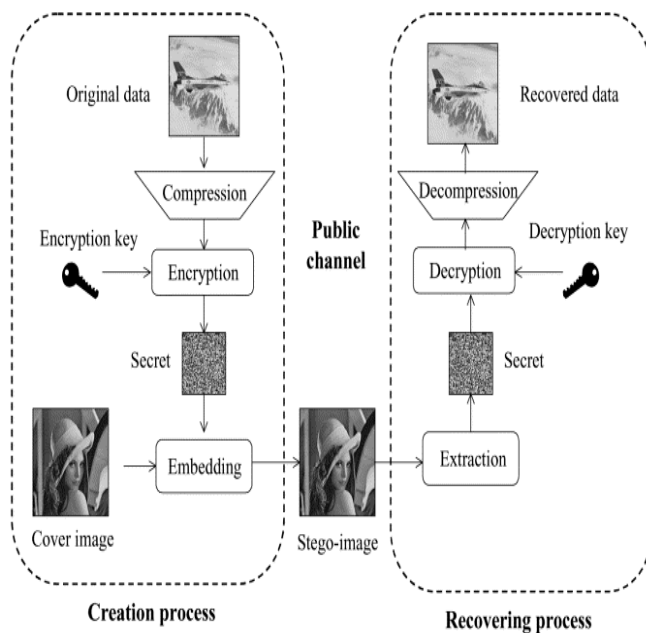


Figure 4 :An Example of the Proposed System Using Image as both Cover-Medium and Data File

2. Embedding Module:

The compressed encrypted Secret Image is embedded in a Cover-Image resulting in the formation of Stego-Image.

3. Extraction Module:

The compressed encrypted Secret Image is extracted from the Stego-Image.

4. Decryption and Decompression Module:

The compressed encrypted Secret Image thus extracted is decrypted using 128 /192/256 AES decoding algorithm and finally it is decompressed if it was compressed earlier.

PROPOSED ALGORITHM

The proposed algorithm can be divided into two main parts:

(i) Encoding Algorithm

Input:

- (i) A Cover-Image (jpg, gif, bmp, tiff, png)
- (ii) A Secret-Image (jpg, gif, bmp, tiff, png)
- (iii) Secret key (16/24/32 byte password)

Output: Stego-Image(jpg, gif, bmp, tiff, png)

Steps:

1. Define the following specifications:
 /*** *Header description (In bytes):* 2(Size of Cover-Image) + 3(Version of the Software) + 1(Features) + 1(Compression Ratio) + 4(Size of Data-File) = 2+ 9 Bytes. *****/
2. Set Version Bytes
3. Set Features Bytes: Three letters indicate-
 UUI (Uncompressed Unencrypted Image) = 0;
 UEI (Uncompressed Encrypted Image) = 1;
 CUI (Compressed Unencrypted Image) = 2;
 CEI (Compressed Encrypted Image) = 3;
4. Set Offset and Header length
 OFFSET_JPG= 3;
 OFFSET_PNG= 42;
 OFFSET_GIF_BMP_TIF= 32;
 HEADER_LENGTH= 15* 4;
5. Bring Cover Image in the Buffer.
6. Create Stego-Image in the Buffer and write to it upto OFFSET bytes from the buffered Cover-Image.
7. Embed Cover-Image size to the buffered Stego-Image. Write the remaining Cover-File to the buffered Stego-Image.
8. Embed version information into the buffered Stego-Image.
9. Write features information into the buffered Stego-Image.
10. Bring the Secret-Image in the Buffer.

11. Compress the buffered Secret-Image if required according to the requirement i.e., high level or low level.
12. Embed compression ratio into the buffered Stego-Image.
13. Encrypt the buffered Secret-Image using AES 128/192/256 bit key.
14. Embed buffered Secret-Image size in the buffered Stego-Image.
15. Embed buffered Secret-Image into the buffered Stego-Image.
16. Write buffered Stego-Image to the disk.

(ii) Decoding Algorithm

Input:

- (i) Stego-Image(jpg, gif, bmp, tiff, png)
- (ii) Secret key(16/24/32 byte password)

Output: Secret Image (jpg, gif, bmp, tiff, png)

Steps:

1. Bring Stego-Image in the Buffer.
2. Obtain the Cover-Image length(size). Retrieve remaining of the Cover-Image information.
3. Retrieve the name and version information.
4. Obtain the features.
5. Obtain the compression ratio.
6. Obtain the Secret-Image length (size).
7. Obtain the encrypted compressed Secret-Image from the Stego-Image.
8. Get secret key and Decrypt the Secret-Image using AES 128/192/256 decryption algorithm to obtain compressed Secret-Image.
9. Uncompress the Secret-Image.
10. Write the retrieved Secret-Image to the disk.

VI. RESULTS

The above system was developed and tested using the following standard images: Babara.bmp as the Secret-Image and Lena(jpg ,gif, bmp, tiff) as Cover-Images. The results are as listed in Table 1.












It can be seen that the PSNR values obtained is varies in the range of 90-99%.So it can be concluded that the original Secret-Image and the retrieved Secret-Image are almost alike.

VII. CONCLUSION

Steganography, especially combined with the cryptography is a powerful tool which enables to communicate secretly. The developed system provides a high level of secrecy and security and allows a large amount of information to be embedded in Cover-Image as compared with other existing systems. It also allows Zipped Compression and encryption using AES 128/192/256 bit key.

Table 1: Testing Results

S r. N o .	Cover Image and Secret Image	Stego Image Obtained (Cover Image+Secret Image) (512×512)	Retrieved Secret Image (720×526) Size=1.18 Mb	Comparison between Original Cover Image and Stego Image	Comparison between Original Secret Image and Retrieved Secret Image
1	<p>Cover Image (512×512)</p>  <p>Lena.jpg (67.5 Kb)</p> <p>+</p> <p>Secret Image (720×526)</p>  <p>Barbara.bmp(1.18 Mb)</p>	<p>Low Comp. (1.25 Mb) High Comp. (1.10 Mb)</p>   <p>AES 128 bit</p>   <p>AES 192 bit</p>   <p>AES 256 bit</p>	<p>Low Comp. (1.18 Mb) High Comp. (1.18 Mb)</p>   <p>AES 128 bit</p>   <p>AES 192 bit</p>   <p>AES 256 bit</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio =99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: Statistics remains the same for case:1ai to case:1cii</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio= 99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: Statistics remains the same for case:1ai to case:1cii</p>
2	<p>Cover Image (512×512)</p>  <p>Lena.gif(222 Kb)</p> <p>+</p> <p>Secret Image (720×526)</p>  <p>Barbara.bmp(1.18 Mb)</p>	<p>Low Comp. (1.40 Mb) High Comp. (1.25 Mb)</p>   <p>AES 128 bit</p>   <p>AES 192 bit</p>	<p>Low Comp. (1.18 Mb) High Comp. (1.18 Mb)</p>   <p>AES 128 bit</p>   <p>AES 192 bit</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio =99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: Statistics remains the same for case:2ai to case:2cii</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio= 99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: Statistics remains the same for case:2ai to case:2cii</p>

		 <p style="text-align: center;">AES 256 bit</p>	 <p style="text-align: center;">AES 256 bit</p>		
3	<p>Cover Image (512x512)</p>  <p>Lena.tiff(768 Kb)</p> <p style="text-align: center;">+</p> <p>Secret Image (720x526)</p>  <p>Barbara.bmp(1.18 Mb)</p>	<p>Low Comp. (1.93 Mb) High Comp. (1.78 Mb)</p>  <p style="text-align: center;">AES 128 bit</p>  <p style="text-align: center;">AES 192 bit</p>  <p style="text-align: center;">AES 256 bit</p>	<p>Low Comp. (1.18 Mb) High Comp. (1.18 Mb)</p>  <p style="text-align: center;">AES 128 bit</p>  <p style="text-align: center;">AES 192 bit</p>  <p style="text-align: center;">AES 256 bit</p>	<p>Mean Square Error = 4.5776e-05</p> <p>Peak Signal to Noise Ratio = 91.5244</p> <p>Normalized Cross-Correlation = 1.0000</p> <p>Average Difference = 3.0518e-05</p> <p>Structural Content = 1.0000</p> <p>Maximum Difference = 2</p> <p>Normalized Absolute Error = 2.4603e-07</p> <p>Remark: Statistics remains the same for case:3ai to case:3cii</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio= 99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: Statistics remains the same for case:3ai to case:3cii</p>
4	<p>Cover Image (512x512)</p>  <p>Lena.bmp(768 Kb)</p> <p style="text-align: center;">+</p> <p>Secret Image (720x526)</p>  <p>Barbara.bmp(1.18 Mb)</p>	<p>Low Comp. (1.93 Mb) High Comp. (1.78 Mb)</p>  <p style="text-align: center;">AES 128 bit</p>  <p style="text-align: center;">AES 192 bit</p>	<p>Low Comp. (1.18 Mb) High Comp. (1.18 Mb)</p>  <p style="text-align: center;">AES 128 bit</p>  <p style="text-align: center;">AES 192 bit</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio= 99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: i.Statistics remains the same</p>	<p>Mean Square Error = 0</p> <p>Peak Signal to Noise Ratio= 99</p> <p>Normalized Cross-Correlation = 1</p> <p>Average Difference = 0</p> <p>Structural Content = 1</p> <p>Maximum Difference = 0</p> <p>Normalized Absolute Error = 0</p> <p>Remark: Statistics remains the same for</p>

	Mb)	 <p style="text-align: center;">AES 256 bit</p>	 <p style="text-align: center;">AES 256 bit</p>	for case:5ai to case:5cii ii. Thumbnails can be seen properly but Stego image gets distorted when previewed.	case:5ai to case:5cii
--	-----	----------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------	-----------------------

REFERENCES

- Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath, "Evaluating image Steganography techniques: Future research challenges", *Computing, Management and Telecommunications (ComManTel), 2013 International Conference*, ISBN:978-1-4673-2087-0, Jan. 2013.
- Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984)
- Moerland, T, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/trnoerl/privtech.pdf.
- T Morkel, J.H.P Eloff, M.S Olivier, "AN OVERVIEW OF IMAGE STEGANOGRAPHY". Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), 2005.
- Birgit Pitzmann, "Information hiding terminology-results of an informal plenary meeting and additional proposals", Proc. of the First International Workshop on Information Hiding, vol. 1174, pp.347-350. Springer, 1996.
- Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, "Security Improvisation in image Steganography using DES", 3rd IEEE Trans. International Conference IACC -2013, Page(s): 1094 – 1099.
- Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, Monika Sharma "Image Stenography: Self Extraction Mechanism", UACEE International Journal of Advances in Computer Science and its Applications- IJCSIA Vol -3 Issue -2, ISSN 2250-3765 Pg-145-148, 2013.
- Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, "Improvisation of Security Aspect in Steganography Applying DES", 2013 International Conference on Communication Systems and Network Technologies, ISBN: 978-0-7695-4958-3/13, Page(s): 431 – 436.
- Federal Information Processing Standard Publication (FIPS 197), "Advance Encryption Standard (AES)", 26 Nov. 2001.
- "Steanograph 1.0.0" by Muhammad Muneez & "Secure Chat" by Muhammad Muneez
- Yambin Jina Chanu, Themrichon Tuithung, Kh Manglem singh, "A Short Survey on Image Steganography and Steganalysis Technique", IEEE Trans. 2012
- Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Parta Pratim Sarkar "An Image Steganography Technioque using X-Box Mapping", IEEE Trans. International Conference Advances in Engineering, science and Mamage (ICAESM- 2012) 709 -713.
- Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing, (2011) 252-255.
- W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forensic Security 5 (2) (2010) 201-214.
- Guiliang Zhu, Weiping Wang, "Digital Image Encryption algorithm based on pixel", ICIS – 2010 IEEE International Conference 29-31 Oct 2010, pp – 769 – 772.
- Jasmin Cosic, Miroslav Bacai, "Steganography and Steganalysis Does Local web Site contain "Stego" Contain", 52 th IEEE Trans. International Symposium ELMAR-2010, Zadar, Croatia 2009 , pp 85 – 88.
- Zhang Yun-peng , Liu Wei " Digital Image Encryption Algorithm Based on chaos and improved DES ", System, man and Cybernetics ,SMC 2009 , IEEE International Conference 11-14 Oct 2009, pp 474-479.
- J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287.
- Saeed R. Khosravirad, Taraneh Eghlidos and Sharokh Ghaemmaghami, "Higher Order Statistical of Random LSB Steganography", IEEE Trans. 2009, pp 629 - 632.
- N Provos and P. Honeyman, "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy, 2003, pp32-44.
- Donovan Artz " Digital Steganography: Hiding Data within Data ", Los Alamos National Laboratory, IEEE Trans. 2001, pp 75-80.
- Schaefer " A Simplified Data Encryption Standard Algorithm ", Cryptologia, January 1996