



RESEARCH ARTICLE

4-LEVEL ENCRYPTION USING DWT IN IMAGE STEGANOGRAPHY

Ms. Souma Pal and *Prof. Samir Kumar Bandyopadhyay

Computer Science and Engineering, University of Calcutta, India

ARTICLE INFO

Article History:

Received 29th June, 2017
Received in revised form
17th July, 2017
Accepted 09th August, 2017
Published online 30th September, 2017

Key words:

DWT, Hebb Rule,
Weight Adjustment,
XOR operation,
LSB Substitution Method.

ABSTRACT

Data and information are spread all over the world. So the secrecy of data is important to our digital world. To maintain the secrecy of data, two efficient approaches are introduced- Cryptography and Steganography. Steganography is the science that deals with conveying secret information by embedding into the cover object invisibly. In steganography, only the authorized party is aware of the existence of the hidden message to achieve secret communication. The message that is to be hidden and the cover medium where the message is hidden may be text, image, audio, video and protocol. In this paper, data (ASCII range 0-255) is embedded within an image (jpg,pgm,png or tiff) by implementing DWT using Hebb rule. Then LSB substitution method is for transmission only the stego-image file and follows the reverse procedure to decrypt the original data.

Copyright©2017, Ms. Souma Pal and Prof. Samir Kumar Bandyopadhyay. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Citation: Ms. Souma Pal and Prof. Samir Kumar Bandyopadhyay. 2017. "4-Level Encryption Using DWT in Image Steganography.", *International Journal of Current Research*, 9, (09), 58103-58109.

INTRODUCTION

Steganography is a procedure of "secret or protected writing". Its meaning is derived from Greek term, "Steganos" refers to —covered or protected and "graphei" means —writing. So Steganography is an art of secret writing in which any length of confidential information (may be text, audio, video, image and so on) are concealed within a cover medium (may be text, audio, video, image and so on) in such a way so that malicious users' eyes cannot catch it, only the intended receiver (s) is/are aware of the existence of the valuable information and they can only decrypt it. There are various types of Steganography according to the nature of embedded medium like text, image, audio, video Steganography etc. Discrete Wavelet Transformation (DWT) is an efficient mathematical tool of processing the digital image with multiple resolutions. It is a class of powerful, unique but related transformations that differ not only in the transformation kernels employed (the expansion functions) but also fundamental nature of those functions and their application to disclose insight into an image's spatial and frequency characteristics. The DWT can identify portions of cover image where secret data could be effectively hidden. DWT splits information into its high and low frequency components.

The high frequency part of the signal contain details about the edge components, whereas the low frequency part contains most of the signal information of the image which is again split into higher and lower frequency parts. For each level of decomposition in two dimensional applications, first DWT is performed in the vertical direction followed by horizontal direction. For a Neural Net, the Hebb Learning Rule is simple one. According to the Hebb rule, the weight vector is found to increase proportionately to the product of the input and the learning signal. Here the learning signal is equal to the neuron's output. The weight updating formula can also be given in vector form as, $w(\text{new}) = w(\text{old}) + xy$, Here the change in weight can be expressed as $\Delta w = xy$. As a result, $w(\text{new}) = w(\text{old}) + \Delta w$. In this paper, The Hebb learning rule is applied to hide the original information and to get the new information in which the input bit string is represented as a $w(\text{old})$, x is the column value of the corresponding bit information and y is the sign value of the every DWT value.

Review Works

DWT is another frequency domain in which steganography can be implemented. CT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is removed using DWT. DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact.

*Corresponding author: Prof. Samir Kumar Bandyopadhyay
Computer Science and Engineering, University of Calcutta, India

LIU Tong *et al.* proposed a DWT based colour image steganography method. In the former method the secret information is hidden into a publicly accessed colour image by quantization-based strategy (Liu, 2002). Whereas, the latter case method processes grey scale images as cover object for creating subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete transform for embedding process. Artz, D. proposed steganography and its implementation techniques (Artz, 2001). Deshpande Neeta *et al.* proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file (Deshpande Neeta, 2004). Ali Al-Ataby *et al.* proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security (Ali Al-Ataby, 2010). T. Narasimmalou *et al.* proposed a new image data hiding technique based on discrete wavelet transform (Narasimmalou, 2012). The stego image is looking perfectly intact and has high peak signal to noise ratio value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image. H.J. Patel and Dave have proposed a new variant of LSB based image steganography (Patel, 2012). In this, both the parties will have to agree upon a set of carrier images and certain required parameters. Then the sender will select an image, from the set of carrier images which requires least number of bit manipulations on LSB substitution of secret data, and produce stego image. Then the receiver on receiving stego image will extract LSBs along with the help of the received parameters. The probability of guessing parameters is very less. So extraction without those parameters is very difficult. Here since both the parties agree upon a set of carrier images the visual difference between stego image and original image can be reduced. T. Narasimmalou *et al.* proposed an optimal discrete wavelet transform (DWT) based steganography (Narasimmalou, 2012). Experiments represent that the peak signal noise ratio (PSNR) generated by the proposed method is better. Ashok Kumar *et al.* proposed biometric steganography that uses skin region of images in DWT domain for embedding secret data (Ashok Kumar Balijepalli, 2012). By embedding data in only specific region (here skin region) and not in whole image security is enhanced. Also image cropping concept introduced which maintains security at respectable level since no one can extract message without having value of cropped region. Features obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. Mahajan *et al.* proposed a secure image steganographic model using RSA algorithm and LSB insertion (Tiwari, 2012). In this method, the secret data is first encrypted using recipient's RSA public key. Then each bit of the encrypted message is inserted to the LSBs of image in different images so as to find the best cover image. Best cover image is the one which requires minimum number of LSB extract the message in the encrypted form and will decrypt it using private key. Stuti Goel *et al.* proposed the performance and comparison of three techniques DCT, LSB & DWT is evaluated on the basis of the parameters MSE, PSNR, Capacity & Robustness (10). From the results, it is clear that PSNR of DCT is high as compared to the other two techniques. This implies that DCT provides best quality of the image.

DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security. For images, the JPEG images are taken into account as it preferred DWT over DCT or DFT (Sonja Grgic, 2001). In DFT, execution time is lower and it provides lower compression as compared to the other techniques. In DCT is simple compression algorithm, because computation count in this algorithm is limited, hence provides lower compression ratio. DWT on the other hand, is complex and computation count is very high and it provides higher compression ratio as compared to later two and also proven to be more effective. In wavelet transform system the entire image is transformed and compressed as a single data object rather than block by block as in a DCT based compression system. It can provide better image quality than DCT, especially on higher compression ratio. After preliminary study of literature based on these compression techniques we evaluated that DWT with HAAR Wavelet is the best performer among all other compression techniques available in our selection in terms of compression ratio and elapsed time. Finally, the decision is made to use DWT for its effectiveness and robustness over DCT and DFT (Stuti Goel, 2013; Xiangui Kang and Jiwu Huang, 2003).

Proposed Method

This image steganographic method highlights on 4-level encryption technique. At first, read the length of input bit string (ASCII range) and then input a cover image whose size is double of input bit length. The cover image is divided into two parts, i.e., if the image size is 256X256, the size of each part will be 256X128. Now calculate DWT of 2nd block of the image. A new bit string is obtained from calculating old bit string, column value and sign value of every DWT value according to Hebb rule. The sign value of new bit string are loaded into a matrix and then adjust the new bit string value so that it becomes binary. Then XOR operation is performed between two matrices and finally embeds the bit value of the matrix which contains sign value at 1st bit position of a pixel and the bit value of the matrix containing bit value after the XOR operation at LSB or 0th position of same pixel of 1st block of the cover image. Lastly, two blocks of the image are merged and thus the stego-image is obtained. This stego-image is transmitted over the network. The intended recipient (s) receive (s) the stego-image and decrypts the reverse procedure to get the original information.

Encrypted Procedure

1. Read a gray image as the cover image and calculate its size.
2. Split the image into two blocks and calculate the size of each block.
3. Calculate Discrete Wave Transform (DWT) of 2nd block.
4. Pick up sign values of all DWT into a matrix say y. If $y(i,j) = 0$, then set $y(i,j) = 1$.
5. Calculate how many bits are embedded within the cover image, i.e., no. of bits = size of the image/2.
6. Input binary data stream and the length of the stream must be no. of bits/2.
7. Apply the Hebb rule, i.e., $w_{new}(i,j) = w_{old}(i,j) + x_i * y(i,j)$ where $w_{new}(i,j)$ = New weighted matrix, $w_{old}(i,j)$ = Old (inputted) weighted matrix, x_i = The column vector and $y(i,j)$ = Sign values of DWT.

8. Adjust the new weights of the matrix (wn) so that every value of the matrix becomes binary and its sign are loaded into another matrix (b). Here payload is 2.
9. Then new weighted matrix (wn) and the matrix containing sign value (b) are xored for better security.
10. Now the bit value of new weighted matrix after xor operation and the bit value of the matrix containing sign values are embedded at LSB or 0th bit position and 1st bit position accordingly into 1st block of the cover image.
11. Merge two blocks and finally obtain the stego image.
12. Lastly, transmit the stego image and the value of payload and length of string as encrypted form.

Encrypted Algorithm

1. Read a gray cover image and resize it (if necessary like 256X256, 512X512 etc.) and then calculate its size.
2. Split the image into two blocks. 1st block is used for embedding and 2nd block is used for calculating DWT.
3. Calculate DWT for 2nd block of the image.
4. Pick up sign values of all DWT values (if sign value is 0, assign 1) and save into a matrix y.
5. Calculate maximum size of bits to be embedded.
6. Level-1 encoding: apply Hebb rule .
 - a) Read a null matrix say wnew.
 - b) Set k:=1 and l:=1.
 - c) for i=1 to len do(len= no. of bits/no. of column)
 - d) for j=1 to 8 do(no. of column=8)
 - e) Set wnew (i,j) :=wold (i,j) +j*y (k,l) ;
 - f) if l<cb then
Set l:=l+1.
- else
Set k:=k+1.
Set l:=1.
(End of if-else structure.)
(End of for loop structure.)
(End of for loop structure.)
7. Level-2 encoding: The weights are adjusted for converting binary and sign values are saved into matrix.
 - a) Read two null matrix b (store sign values) and wn (store new weights)
 - b) for i:=1 to len do
 - c) for j:=1 to 8 do
 - d) Set num:=decimal to binary conversion of wnew (i,j) .
 - e) Set rm:=num%10.
 - f) Set wn (i,j) :=rm.
 - g) if wnew (i,j) >=1 then
 - h) Set b (i,j) :=0.
- Else
Set b (i,j) :=1.
(End of if-else structure.)
(End of for loop structure.)
(End of for loop structure.)
8. Level-3 encoding: Perform XOR operation between new weighted matrix (wn) and sign value (b) matrix.
9. Level-4 encoding: The bit of new weighted matrix after XOR operation and sign bit are embedded into 0th and 1st bit position of a pixel accordingly.
10. Merge two blocks.
11. Finally, the stego-image is obtained and transmitted.

Decryption Procedure

1. Read a graystego image and calculate its size.

2. Split the image into two blocks and calculate the size of each block.
3. Calculate Discrete Wave Transform (DWT) of 2nd block.
4. Pick up sign values of all DWT into a matrix say y. If y (i,j) =0, then set y (i,j) =1
5. Decrypt the embedded data bits from 0th or LSB position and sign values from 1st position of same pixel of 1st block of the stego image.
6. Perform XOR operation between embedded data bits and sign values and stores the results of XOR operation into a matrix.
7. The weights are adjusted using the values of the resultant matrix and sign values matrix.
8. Follow the reverse procedure to get back the original data stream.







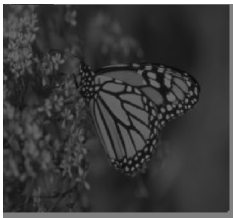
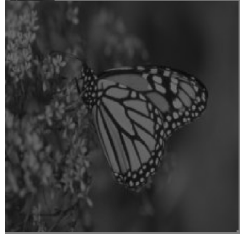
Decrypted Algorithm

1. Read the stego image and calculate its size.
2. Split the image into two blocks. 1st block is used for decryption and 2nd block is used for calculating DWT.
3. Calculate DWT for 2nd block of the image.
4. Pick up sign values of all DWT values (if sign value is 0, assign 1) and save into a matrix y.
5. Decrypt the embedded data bits from 0th or LSB position and sign values from 1st position of same pixel of 1st block of the stego image.
6. Perform XOR operation between embedded data bits and sign values and stores the results of XOR operation into a matrix.
7. The weights are adjusted reversely.
 - a) Read a null matrix wnew and u.
 - b) Set k:=1.
 - c) Set v:=(1, 1, 0, 0).
 - d) for i:=1 to len do
 - e) for j:=1 to 8 do
 - f) Set u (1,k) := (-1) * (j-1) .
 - g) Set u (1,k+1) := (-1) *j.
 - h) Set u (1,k+2) :=j.
 - i) Set u (1,k+3) :=j+1.
 - j) for k:=1 to 4 do
 - k) Set num:=decimal to binary conversion of u (1,k) .
 - l) Set rm:=num%10.
 - m) if wn (i,j) =rm & v (1,k) =b (i,j)
Set wnew (i,j) :=u (1,k) .
Break.
(End of if structure.)
(End of for loop structure.)
 - n) Set u:=() and Set k:=1.
(End of for loop.)
(End of for loop.)
8. Get back original data.
 - a) Read a null matrix say wback.
 - b) Set k:=1 and Set l:=1.
 - c) for i:=1 to len do
 - d) for j:=1 to 8 do
 - e) Set wback (i,j) :=wnew (i,j) -j*y (k,l) .
 - f) if l<cb then
Set l:=l+1.
- else
Set k:=k+1.
Set l:=1.
(End of if-else structure.)
(End of for loop structure.)
(End of for loop structure.)



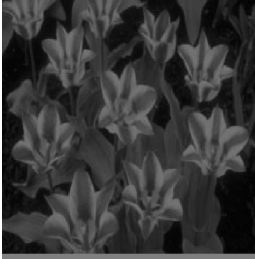

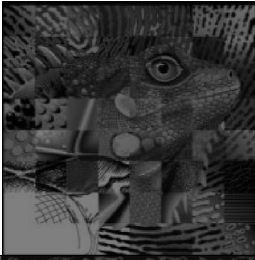


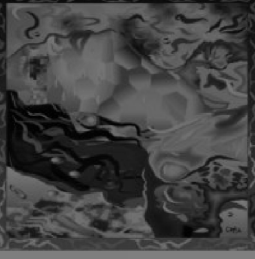

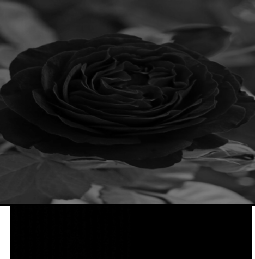
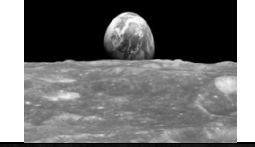
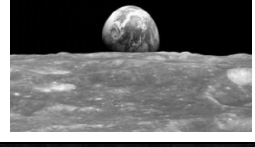
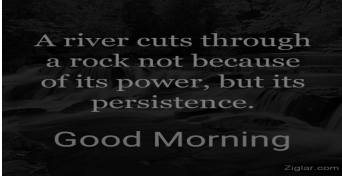
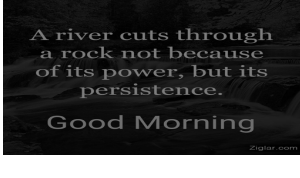
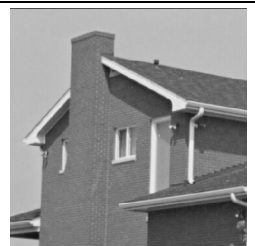
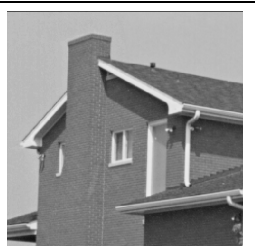
Name of the Image file	Resolution of the image	No.of input bits embedded	No. of total bits embedded	PSNR	MSE
Aerial.pgm	256X256	4KB	16KB	47.1273	1.2599
Lena.pgm	512X512	16KB	32KB	47.1609	1.2502
Peppers.pgm	512X512	16KB	32KB	47.1561	1.2516
Monarch.png	512X512	16KB	32KB	46.9961	1.2986
Clegg.png	512X512	16KB	32KB	47.0912	1.2705
Sail.png	512X512	16KB	32KB	47.1360	1.2574
Tulips.png	512X512	16KB	32KB	47.0671	1.2775
Frymire.png	512X512	16KB	32KB	47.0161	1.2926
Serrano.png	512X512	16KB	32KB	47.0258	1.2897
Rose.jpg	512X512	16KB	32KB	47.1661	1.2487
Earth.jpg	256X256	4KB	16KB	47.4421	1.1718
Scenary.jpg	512X512	16KB	32KB	47.1606	1.2503
Jellybeans.tiff	256X256	4KB	16KB	47.2210	1.2330
House.tiff	256X256	4KB	16KB	47.0922	1.2702
Aeroplane.tif	512X512	16KB	32KB	47.1636	1.2495
Romancandy.png	512X512	16KB	32KB	47.1289	1.2595
Pigeon.png	256X256	4KB	16KB	47.2821	1.2158
Guitar.png	512X512	16KB	32KB	47.6543	1.1160

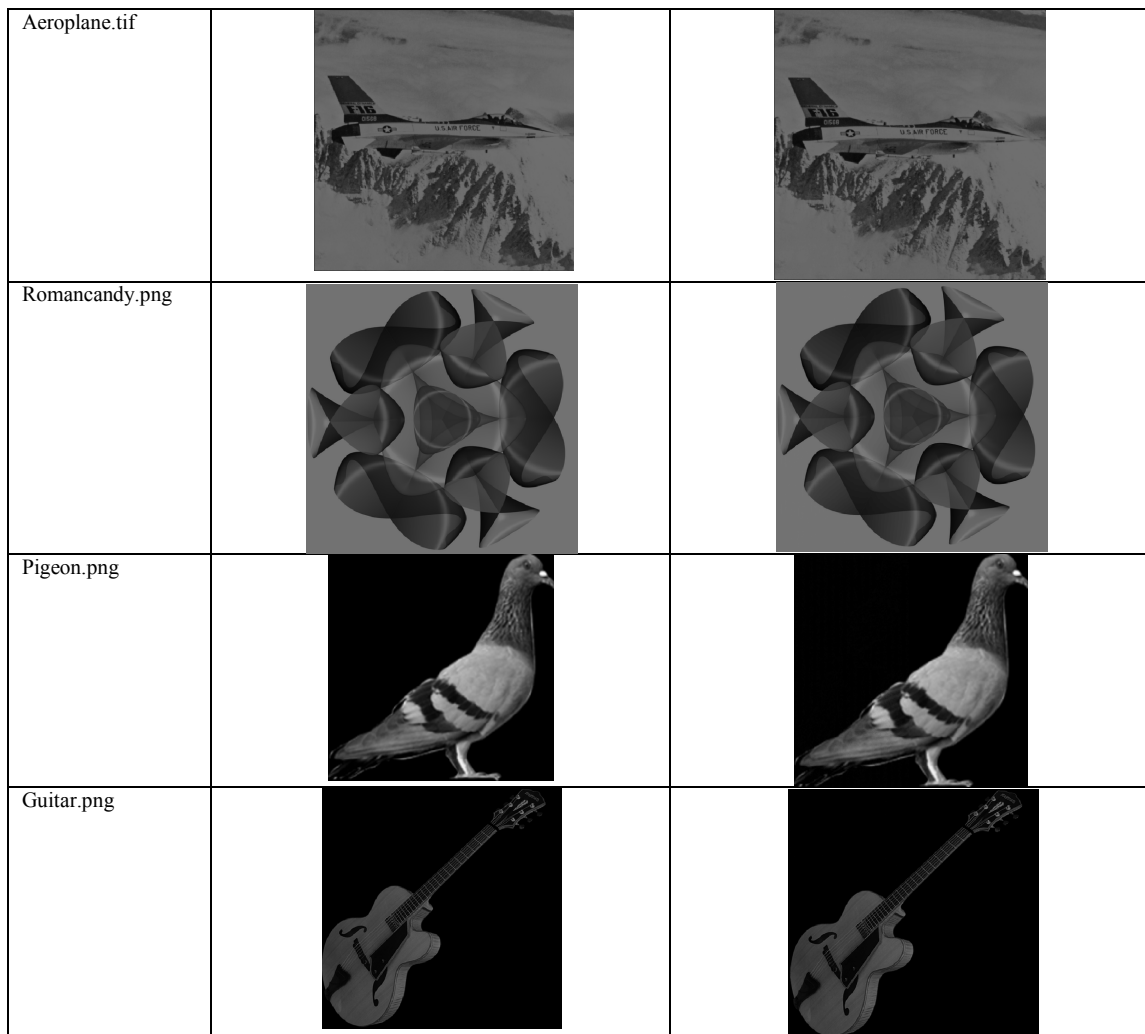
Name of the image file	Proposed Work	Related Work
	PSNR Value	PSNR Value
Lena	47.1609	54.4378
Monarch	46.9961	54.5596
Peppers	47.1561	56.1197
Tulips	47.0671	55.1921
Clegg	47.0912	56.0077
Frymire	47.0161	55.9184
Sail	47.1360	54.9883
Serrnao	47.0258	56.3943

Cover image and stego image

Image file	Cover image	Stego image
Aerial.pgm		
Lena.pgm		
Peppers.pgm		
Monarch.png		

Continue

Sail.png		
Tulips.png		
Frymire.png		
Serrano.png		
Rose.jpg		
Earth.jpg		
Scenary.jpg		
House.tiff		



RESULTS AND DISCUSSION

Our proposed method can be applied any kind (jpeg,png,tiff) of any size of image and then resize it like 256X256, 512X512, 1024X1024 and so on as the cover image as per requirement. Half of image size of binary data can be embedded within the cover image. But the payload (No.of bits embedded within a pixel,i.e. out of 8 bits 2 bits are embedded) of this method is two or $\frac{1}{4}$, 0th or LSB of a pixel is used to store data and 1st bit of same pixel is used to store sign value of data. Here, the spatial domain are used for embedding by using DWT as transform domain and Hebb rule and no extra memory space are required to store information. Only the stego-image are transmitted via network. The extraction procedure is easy but efficient to decode the actual data from stego-image. The PSNR of stego-image is average 47.

Conclusion

This paper work is related with 4-level image steganography technique using discrete wavelet transform (DWT) domain, Hebb rule, XOR operation and lastly spatial domain encryption. The extraction procedure is simple and efficient. This method maintains the prime objective of steganography, which is the secrecy. The stego image preserves the visible quality of original cover image. This method succeeds to keep intact the original image, after the extraction of embedded secret message. Hence this proposed method can be termed as successful new technique of image steganography.

REFERENCES

- Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on WaveletTransform". The International Arab Journal of Information Technology, 2010.
- Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing,2001.
- Ashok Kumar Balijepalli, L. 2012. Srinivas, Niet and Kantepudi"steganography based secrete communicationusing dwt" International Journal of Engineering Research & Technology.
- Deshpande Neeta, KamalapurSnehal, and Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for VariousBits", 2004.
- Liu, T. and Qiu, Z. 2002. "A DWT-Based Color Image Steganography Scheme," in Proc. IEEE, 6th *International Conference onSignal Processing*.
- Narasimmalou, T. and Allen Joseph, R. 2012. "Discrete Wavelet Transform Based Steganography for Transmitting Images". IEEEInternationalConference onAdvances in Engineering, Science and Management, CAESM, 2012.
- Narasimmalou, T. and Allen Joseph, R. 2012. "Optimized Discrete Wavelet Transform based Steganography", IEEE InternationalConference on Advanced Communication Control and Computing Technologies (ICACCCT) .
- Patel, H. J. and Dave, P. K. 2012. "Least Significant Bits Based Steganography Technique," in Proc. IJECCE.
- Sonja Grgic and MislavGrgic, 2001. "Performance Analysis of Image Compression Using Wavelets", ITIE.

- StutiGoel, Arun and Rana, Manpreet Kaur, 2013. "A Review of Comparison Techniques of Image Steganography". IOSR *Journal of Electrical and Electronics Engineering*, (IOSR-JEEE).
- Tiwari, S., Mahajan, R.P. and Shrivastava, N. 2012. "Steganography-an Approach for Data Hiding Based on Encryption and Lsb Insertion," IJECCE.
- Xiangui Kang and Jiwu Huang, 2003. "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression", ITCSVT.
