# DWT and Modified AES based Secure Image Steganography on ARM A8 Processor

Ravi S P
Dept. of Electronics and Communication Engg.
Bangalore Institute of Technology
Bengaluru, India

Dhanalakshmi L
Dept. of Electronics and Communication Engg.
Bangalore Institute of Technology
Bengaluru ,India

***Abstract***— **Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. The steganography is used for secure communication. In this paper we propose a Discrete Wavelet Transform (DWT) based high capacity steganography using coefficient replacement with increased security by adapting an encryption of payload Image. The Haar and biorthogonal DWT is applied separately on cover image and Advanced Encryption Standard (AES) with modification is applied on payload to convert payload image into an encrypted image. The resulted coefficients of payload image are embedded inside the high frequency bands of cover image. The new concept of replacing HH sub band coefficients by encrypted payload is introduced to generate intermediate stego image. It is observed that the capacity and security are increased in the proposed algorithm compared to existing algorithms. The algorithm is finally tested on ARM8 processor.**

***Keywords---Advanced Encryption Standard (AES),Discrete Wavelet Transform (DWT), Hiding capacity, Secured Image steganography.***

## I. Introduction

Encryption is absolutely vital to the security of all digital communications on the Internet. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. It is high security technique for long data transmission. . In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol.

The steganography is categorized into: Spatial domain steganography which mainly includes LSB steganography and Bit Plane Complexity Segmentation (BPCS) algorithm. Spatial methods are the frequently used steganographic techniques because of high capability of hidden information and easy realization. Transform domain steganography in which secret information is embedded in the transform coefficients. Discrete Cosine Transform, Discrete Wavelet Transform and Discrete Fourier Transform are examples of transform domain. The advantages of transform domain techniques are high ability to tolerate noises and some signal processing operations.

Steganography has to satisfy two requirements, one is capability and the other is transparency. Capability means embedding large payload into media. Transparency indicates an ability to prevent distinctions between stego and cover image by perceptual or statistical analysis.

S.Thenmozhi and Chandrasekaran, [1] proposed a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain..First the henon mapping (chaos) is applied on the secret image and the two dimensional Discrete Wavelet Transform (2-D DWT) is performed on the cover image of size MxN. Then each bit of scrambled image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. The experimental results show that the algorithm has a high capacity and a good invisibility. JaspalKaurSaini and Harsh K Verma, [2]proposed the hybrid approach for image security that combines both encryption and steganography. First the image is encrypted using proposed new version of AES algorithm, which is then hided into cover image using the steganography concept. This hybrid approach provides greater security against attacks.

Mohammad Reza DastjaniFarahani and Ali Pourmohammad, [3] proposed a Discrete Wavelet Transform (DWT) steganography method is presented. First, the message data and the cover image data are transformed using Haar filters based DWT, and then, the message DWT coefficients are embedded to the cover image DWT coefficients. The robustness and image brightness are considered as the main criteria. Hence, the PSNR is considered as an objective criteria and the image brightness is considered as a subjective criteria for evaluation. SalehSaraireh, [4] proposed a secure communication system. It employs cryptographic algorithm together with steganography. In this paper, the filter bank cipher is used to encrypt the secret text message, it provide high level of security, scalability and speed. After that, a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR) and histogram analysis.Manojgowtham et al, [5] proposed biometric featured steganography. Here secret data is encrypted by AES and embedded within skin region of image that will provide an excellent secure location for data hiding. Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. The work showed that the skin tone objects tracked with higher security and also satisfactory PSNR (Peak Signal-to-Noise Ratio) is obtained.Syedafarhanatasneem et al, [6]proposed a method the plain text is encrypted by using Advanced Encryption Standard (AES) algorithm. The encrypted text is embedded into image using steganographic technique using Discrete Wavelet Transform (DWT) method .VikasKaul, S.K.Narayankhedkar and S.Achekar described the Hybrid based 128-bitkey AES-DES algorithm, [7] to enhance the security of next generation networks The problem with AES, most extensively used encryption, is that it uses many multivariate equations which are linear in nature. Thus it can be broken using algebraic cryptanalysis. This provides a serious threat as AES was considered to be unbreakable and thus it was used in many encryption systems.

In the following ,we dicuss proposed method of steganography using DWT in section IIA and Modified AES algorithm in section IIB, section III SHOWS THE SIMULATION RESULT.IN Section IV performance parameters for steganography are tabulated. Further, proposed method is concluded and future work is mentioned in section V followed by references .

## II. WORKING OF PROPOSED METHOD

In this section, the payload image is embedded in a cover image. The DWT algorithm is applied to the cover image and Modified AES technique is applied to the payload image. The resultant coefficients of payload image are embedded inside the high frequency bands of cover image. The block diagram of proposed model is given in Figure 1 and Figure 2

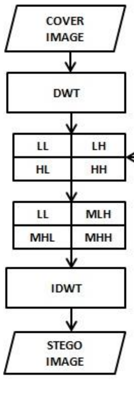


Fig.1 Embedding Algorthim

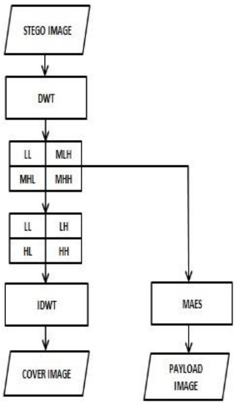


Fig.2 Reconstruction Algorthim

The cover image and payload image of JPG, BMP, TIF, PNG formats with different dimensions are considered to verify the algorithm.

### *A. Discrete Wavelet Transform*

DWT provides sufficient information both for analysis and synthesis of the original image with a significant reduction in computation time .

By applying 2D DWT on an image, the image is decomposed into four sub bands LL, LH, HL, HH sub bands, corresponding to approximate, horizontal, vertical, and diagonal features respectively.

Here, one level DWT is applied on Cover image. Haar wavelet is used as the mother wavelet. Approximate band i.e., LL band is considered as the most significant information of the cover image.

Therefore the Encrypted payload image is embedded in the rest of the 3 bands i.e in LH, HL and HH bands .Each bit of image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform.

### *B. MAES (Modified Advanced Encryption Standard)*

In this, the standard AES algorithm is modified in order to increase the efficiency of encryption and make it suitable for image encryption. The algorithm is basically divided into 11 rounds in which the first round is referred as Add round key stage followed by nine rounds going through six stages of operation called as iteration. The six stages of each iteration is:

1. Sub Bytes
2. Shift Row
3. Mix Column
4. Add Round Key
5. Transpose of a matrix
6. BIT Manipulations

These two additional operations are performed along with Standard AES operation.
Then finally the 10th round which gives the iteration of 3 stages as:

1. Sub Bytes
2. Shift Row
3. Add Round Key

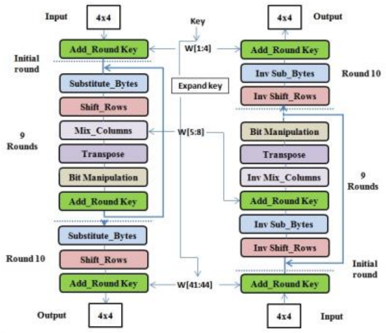


Fig.3 Modified Advanced Encryption Standard algorithm

All the operations are carried out similarly as AES with the addition of Transpose and Bit manipulation operation as shown in Figure 3
1) Transpose of a matrix:
After performing the Mix columns step. Each 4*4 matrix is transposed in order to enhance the security. While decrypting inverse transpose is performed.
2) Bit Manipulations:
The Bit positions are interchanged for the obtained transposed matrix to enhance the security. Figure 4(a),(b) & (c) shows the Input image, AES image & MAES image

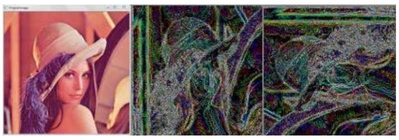
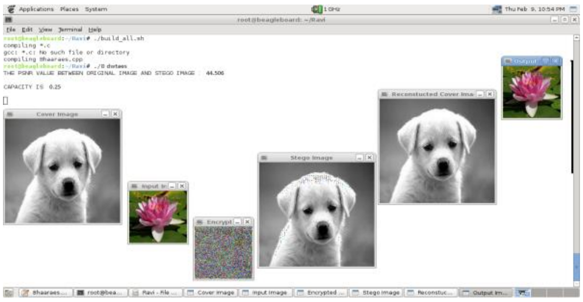


Fig.4 (a) Input image (b) AES (c) MAES image

Stego image is obtained by applying IDWT to the stego coefficients which contains AES encrypted payload image values embedded in the LH, HL and HH bands of the cover image values. The cover image and payload image can be reconstructed by performing the reverse steps.

## III. Simulation Results

Simulations were carried out using OpenCV 2.4.2[11] ,[12 ] & Microsoft Visual Studio 2012 softwares and tested on ARM A8 Processor [10]. Results of PSNR & Capacity are tabulated .Figure 5 showing the simulation output.



```
root@beagleboard:~/Ravi# ./build_all.sh
compiling *.c
gcc: *.c: No such file or directory
compiling Bhaaraes.cpp
root@beagleboard:~/Ravi# ./B dwtaes
THE PSNR VALUE BETWEEN ORIGINAL IMAGE AND STEGO IMAGE : 44.506

CAPACITY IS 0.25
```

Fig.5 Simulation result showing encrypted image ,stego image,reconstructed cover & payload image.

## IV. PERFORMANCE ANALYSIS

The performance parameter PSNR is computed in the same way by using different kinds of images, different sizes. With different techniques such as DWT, DWT+AES and DWT+MAES are discussed in this section. The cover images Lena, Fruit, Barbara and Deer used for the performance analysis are shown in Figure 6.1. The payload images Baby and Lena are shown in the fig 6.2.

(a) (b) (c) (d)

Fig.6.1 The Cover images a)Lena.jpg b)Fruit.jpg c)Barbara.jpg d)Deer.jpg.

(a) (b)

Fig.6.2 The Payload images a)baby.jpg b)Lena.jpg.

The variations of PSNR using DWT, DWT+AES and DWT+MAES for different combinations of Cover and Payload images are tabulated. The PSNR value of proposed technique i.e. DWT+MAES is almost equivalent to existing DWT and DWT+AES techniques. The advantage of proposed technique is the payload encryption is better compared to existing AES algorithm.

TABLE I
PSNR Values for DWT, DWT+AES and DWT+MAES with capacity 0.25

| CI(512*512)/PI(256*256) | DWT | DWT+AES | DWT+MAES |
|---|---|---|---|
| Lena/Fruit | 44.99 | 43.55 | 43.59 |
| Deer/Baby | 44.13 | 43.45 | 43.49 |
| Barbara/Lena | 43.66 | 42.90 | 42.91 |

TABLE II
PSNR Values for different Cover images with a constant Payload image
Payload Image: Lena.jpg(256*256)

| Cover Images (512*512) | PSNR in DB |
|---|---|
| Barbara | 42.9117 |
| Lena | 43.4608 |
| Deer | 43.2106 |

The variations of PSNR with capacity using Biorthogonal wavelet is tabulated in Table III and the corresponding variations are plotted in the fig 7. It is observed that as capacity increases the values of PSNR decreases.

TABLE III
PSNR Values for different Capacity for biorthogonal and Modified AES combination.
Cover Image: Barbara.jpg(512*512) Payload Image: Lena.jpg(different size)

| Payload Image Size | Capacity | PSNR |
|---|---|---|
| 128*128 | 0.0625 | 44.582 |
| 256*256 | 0.25 | 43.689 |
| 320*320 | 0.402 | 41.47 |
| 400*400 | 0.61 | 41.30 |

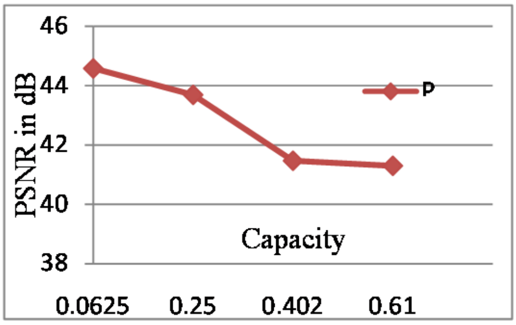


Fig.7 Graphical representation of PSNR v/s Capacity for Biorthogonal and MAES Combination

The variations of PSNR with capacity using Haar wavelet is tabulated in Table 4 and the corresponding variations are plotted in the Figure 8. It is observed that as capacity increases the values of PSNR decreases.

TABLE IV
PSNR Values for different Capacity for HAAR and Modified AES combination,
Cover Image: Barbara.jpg(512*512) Payload Image: Lena.jpg(different size)

| Payload Image Size | Capacity | PSNR |
|---|---|---|
| 128*128 | 0.0625 | 25.26 |
| 256*256 | 0.25 | 24.90 |
| 320*320 | 0.402 | 23.85 |
| 400*400 | 0.61 | 23.30 |

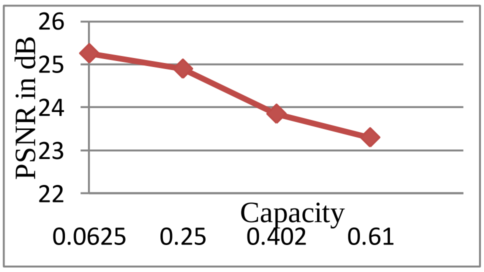


Fig.8 Graphical representation of PSNR v/s Capacity for HAAR and MAES Combination

The PSNR values for the proposed algorithm is compared with existing techniques in table V presented by Mohammed Reza Dastjani[14], Wang Yan[6], Kannimozhi[11] and NehaGupta[13]

Table V
Comparison table of PSNR Values for different proposed technique and existing technique

| Author | Proposed Technique | PSNR values |
|---|---|---|
| Mohammed Reza Dastjani | 2D-Haar DWT | 25.1767 |
| Wang Yan | Spatial Domain | 41.411 |
| Kannimozhi | Coiefflet | 40.8505 |
| Neha Gupta | 1D-Haar DWT | 41.22 |
| Proposed Method | Biorthogonal DWT+MAES | 42.91 |

## V. CONCLUSION

Steganography is a highly useful and predominant method for Image Hiding. The techniques used are highly reliable and are of great use for security purposes. Steganography can be accompanied with other data hiding techniques for extended security. The technology is one of the easiest methods of data hiding and also is one of the most difficult ones to detect.

The work done here on Steganography using 2D-DWT and Modified AES encryption has shown good PSNR and MSE parameters. The MAES encryption has increased the security level preventing access for unauthorized users. The embedding of the payload image inside the cover image resulted in a Stego image that did not have much visual differences from the cover image, making it very difficult for anyone to detect the presence of a hidden message. The retrieved payload image is also obtained without much visual differences from the original secret image.

The algorithm is tested on an ARM A8 processor based beagal board-XM. It is found that the execution speed is same as that of simulation speed.

In future the DWT technique can be replaced by DTCWT technique to enhance security and capacity.

## REFERENCES

(1) S. Thenmozhi and M. Chandrasekaran,“A Novel Technique for Image Steganography Using Nonlinear Chaotic Map”, International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010).

(2) JaspalKaurSaini and Harsh K Verma, “A Hybrid Approach for Image Security by Combining Encryption and Steganography” IEEE Second International Conference on Image Information Processing (ICIIP-2013).

(3) MohammadRezaDastjani,FarahaniandAliPourmohammad,“A DWT Based Perfect Secure and High Capacity Image Steganography Method” International Conference on Parallel and Distributed Computing, Applications and Technologies, 2013.

(4) SalehSaraireh, “A Secure Data Communication System Using Cryptography and Stegnography”,International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

(5) Manojgowtham.G.V, Senthur.T, Sivasankaran.M, Vikram.M and BharathaSreeja.G, “AES BASED STEGANOGRAPHY,” International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2013.

(6) Syedafarhanatasneem,SDurgabhavani and K Suresh babu, “Secure Data Transmission Using Cryptography and Stegnography,” International Conference on Advances in Pattern Recognition, pp. 2009.

(7) VikasKaul, S.K.Narayankhedkar and S.Achekar, “Security enhancement algorithms for data transmissions for next generation networks”, International conference and workshop on recent trends in technology, 2012.

(8) K Kanimozhi, G. Prabakaran and Dr. R. Bhavani, “Dual Transform Based Steganography Using Wavelet Families and Statistical Methods” International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013

(9) Neha Gupta and Nidhi Sharma,“Dwt and Lsb Based Audio Steganography” International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, Feb 2014.

(10) http://beagleboard.org/beagleboard-xm

(11) http://www.intel.com/technology/computing/opencv/index.htm

(12) http://opencvlibrary.sourceforge.net/

**Ravi SP** Pursued B.E. degree in Electronics and Communication Engineering from Global Academy of Technology, Bengaluru, India under Visvesvaraya Technological University, Karnataka, India in 2013. Presently he is pursuing his final year M.Tech with specialization in Digital Electronics and Communication Engineering in Bangalore Institute of Technology (BIT), Bangaluru, Karnataka, India from Visvesvaraya Technological University, Karnataka, India. The proposed research work in this paper is part of his M.Tech thesis.

**L Dhanalakshmi M.E**, Presently she is the Assistant Professor of Electronics and Communication Engineering at Bangalore Institute of Technology (BIT), Bengaluru, Karnataka, India.