Design of an Efficient Steganography Model using Lifting based DWT and Modified-LSB Method on FPGA

Mahesh A.A.1
Associate Professor, Dept. of ECE
PESIT-South Campus, Bangalore, India

Dr. Raja K.B.2
Professor, Dept. of ECE, University Visvesvaraya College of Engineering, Bangalore, India

Abstract—The data transmission with information hiding is a challenging task in today world. To protect the secret data or image from attackers, the steganography techniques are essential. The steganography is a process of hiding the information from one channel to another in data communication. In this research work, Design of an Efficient Steganography Model using Lifting Based DWT and Modified-LSB Method on FPGA is proposed. The stegano module includes DWT (Discrete Wavelet Transformation) with lifting scheme for the cover image and encryption with Bit mapping for a secret image, an embedded module using Modified Least Significant Bit (MLSB) Method, and Inverse DWT to generate the stegano image. The recovery module includes DWT, decoding module with pixel extraction and bit retrievals, and decryption to generate the recovered secret image. The steganography model is designed using Verilog-HDL on Xilinx platform and implemented with Artix-7 Field Programmable Gate Array (FPGA). The hardware resource constraints like Area, time, and power utilization of the proposed model results are tabulated. The performance analysis of the work is evaluated using Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) Ratio for a different cover and secret images with better quality. The proposed steganography model operates at high speed, which improves communication performance.

Keywords—Discrete Wavelet Transformation (DWT); steganography; Modified Least Significant Bit (MLSB) Method; XOR Method; FPGA; cover image; secret image; PSNR; MSE

I. INTRODUCTION

The steganography technique is essential to hide the information in most of the networking and computer applications. The steganography provides security over data alteration, data transmission over secret unsecure channel, and used in digital TV, audio-video synchronization. Steganography is a hiding communication and embeds the hidden content in the cover medium. In general, the stegano medium is the combination of cover medium, stegano key, and embedded message. The different techniques of steganography include text, audio, video, image, and network steganography. The steganography techniques are different from cryptography techniques, because the cryptography converts the overall structure of the data information, whereas in steganography doesn't change the overall structure of the data information [1-3]. There are different ways to classifying steganography methods. Most of the steganography methods hide the information in image files and are classified as spatial domain, spread spectrum, transform domain, statistical, and distortion methods. The Least Significant Bit (LSB) and Pixel Value Difference (PVD) methods are spatial domain methods in image steganography techniques. The spatial domain methods are simple to embed and extract the hidden information, but transformation methods complex compared to spatial domain methods [4-5] [6-7]. The steganography methods are designed and implemented using both software and hardware-based approaches.

Hardware-based approaches are having advantageous over software-based approaches in terms of constraints like less area, less power consumption, and less execution time. The hardware-based steganography approaches meet most of the real-time requirements and used in many applications [8]. The hardware-based approaches provide portability, capable of connecting with other devices, and with low processing speed. The General Purpose Processor (GPP), Digital Signal Processing (DSP), FPGA, and Application Specific Integrated Circuit (ASIC) platforms are available for suitable hardware based steganography approaches. Modern steganography uses FPGA and ASIC platforms; FPGAs are reconfigurable, flexible, and less expensive than ASICs. In this article, the hybrid combination of secured modified LSB and DWT approaches are used to hide the secret image in cover image to generate the stegano image and recover the secret image and also it is implemented on low-cost Artix-7 FPGA.

An efficient steganography technique with stegano and recover module using Lifting based DWT and modified LSB method is designed. Section II describes the review of the existing steganography methods for different applications followed by research gaps. The methodology of the proposed work is overviewed in Section III. The hardware architecture of the proposed stegano and a recovered module is described in Section IV. The resource utilization and performance evaluation concerning PSNR and MSE ratio for different images are represented in Section V. Finally, concludes the overall proposed work with improvements.

II. RELATED WORKS

This section discusses the exhaustive review of the existing steganography techniques with various approaches for different applications in recent years. Kumar et al. [9] presented color image steganography using LSB method with the help of frame deposition technique. The multiple frame video sequences are
used as color image inputs, and component division technique is used to extract the video frames. The architecture is sophisticated and a software-based approach is used for steganography. Desshukh P.U. and T. M. Patelwar [10] presented the LSB method for edge-based steganography. The data hiding and extraction process is done using the edge-based method and analyzes the performance between LSB and edge method. Data hiding is achieved on developed Particle-swarm-optimization (Dev.-PSO) Method using LSB approach by Shakur et al. [11]. The embedding the cover image using Dev.-PSO method and after reconstruct generate the steego image. Apply the inverse of the Dev.-PSO method to a steego image to extract the secret image. Odai et al. [12] presented the Modified LSB method for image steganography with random pixel selection. The hybrid combination of Modified LSB and image segmentation is used before embedding the secret images randomly. Similarly, Abbood et al. [13] presented the Developed LSB and random technique for text in image hiding. The secret text is hidden in the cover image using the random method and use the hash function to hide the secret text in a selected column to generate the steego image. The visible watermarking is applied to the LSB method by Bhatt et al. [14] for image steganography to improve the image quality. Joshi et al. [15] presented the new software-based approach for image hiding and extraction using the 7th bit of pixel replacement by new temporary pixel and also analyze the performance metrics for different images with image quality improvements. Tulsidas et al. [16] present a new way of image steganography by using block division method. The block division method generates the maximum pixel value from each block as key and block wise, divide each pixel by maximum value and embedded with cover to generate the steego image. Perform the average of steego images to extract the secret image. The DWT based steganography method is designed by Sharma et al. [17] for data hiding. In this, hiding the information with a key using cryptographic substitution method and converted to secret image. Apply the cover image with secured secret image message to DWT method to generate the steego image and perform the reverse process using DWT to generate the secret image and convert to text format to get the secret data. Similarly, Shet et al. [18] hide the color image using Integer wavelet transformation approach along with the LSB method. The Ardiansyah et al. [19] presented the hybrid approach with secured triple-DES in secret image and DWT along with LSB method in cover image to generate the secured steego image. The digital watermarking application using image steganography is presented in Chandran et al. [20] using different approaches like Discrete Cosine Transform (DCT), DWT, and LSB methods. Most of the recent image steganography articles from [9-20] are software-based approaches. Almutairi et al. [21] presented the hardware-based steganography using secured LSB method with security, and similarly, the hybrid approach using Haar DWT and Modified LSB method for steganography is made by Simha et al. [22] on a hardware platform. The architecture is so complex and consumed more chip utilization.

Research Gap: After reviewing the existing works, finds the gaps and limitations in the steganography techniques. In that, most of the steganography based methods are based on the software approaches and won’t meet the real-time requirements. Usage of inappropriate spatial or transformation domain usage, which causes computation complexity and leads to low-quality image outcomes. There are only few hardware-based architectures with hybrid approach are available. The proposed work overcomes these gaps with proper methodology and designs.

III. PROPOSED METHODOLOGY

The proposed efficient steganography module using Lifting based DWT and modified LSB method is designed using Verilog-HDL on Xilinx Platform and implemented on Artix-7 FPGA. The schematic flow of the proposed methodology is represented in Fig. 1. Matlab is used only for image representation and binary conversion. Consider the cover and secret image separately, extract the pixel information, and perform the image to binary conversion using Matlab and to generate the cover and secret text files in hex format. The FPGA design of steganography module receives the binary files via test-cases as inputs.

The secret image chosen with the 64x64 size is embedded to cover image of 128x128 size. The secret image data first encrypt using simple XOR method with 8-bit key, and the cover image is applied through lifting-based DWT to generate the high and low pass frequency components. The embedded module operates high pass and low coefficients with encrypted data using the modified LSB Method. Apply the Inverse-DWT to get the 128x128 steego image, which is the embedded version of the cover image with hidden secret image.

The recovery of a secret image is a reverse work of the embedded process. In recover module, the steego image data applied to Lifting based DWT and the generated high-pass component data is fed to decoding module, which extract the pixels and retrieves the bits using LSB method and performs the decryption with the same key for retrieved bits to get back the output text file. Moreover, apply Matlab to convert the text to an image to recover the secret image, which is having a 64x64 image size.

![Fig. 1. Schematic Flow the Proposed Methodology.](image-url)
IV. PROPOSED STEGANOGRAPHY SYSTEM

The Hybrid approach of steganography model includes mainly stegano module and recovery module. The Stegano module consists of Encryption, Bitmapping, splitting with Lifting based DWT, embedded module using the LSB method, and Inverse DWT Module. The Stegano module hardware architecture is represented in Fig. 2. The 128x128 size of cover image stores the pixel’s data in 16384 memory locations, and each location is 8-bits. The splitting module receives the cover data and splits 8-bit even and odd based on the edge of the clock. The even and odd data of 8-bit size are fed to Lifting based DWT Module. The DWT Module uses the lifting based 9/7 filter coefficients on performing predict, update along with scaling and inverse scaling operations. The coefficients are named as alpha, beta, gamma, delta, scaling and inverse scaling. The DWT Module design uses 17-registers, 8-adders, and 4-multipliers for prediction and updating operations.

The prediction operation performs with even data, which is added with a delayed register; the results are multiplied with the filter coefficient (alpha) to generate the predicted data. The updating operation performs with odd data, which is added with predicted data; the results are multiplied with the filter coefficient (beta) to generate the updated data. The same process continues with other filter coefficients gamma and delta which are followed by scaling operation to obtain the 8-bit low-pass component (l) and inverse scaling operation to obtain the 8-bit High-pass component (h).

The 64x64 size of secret image uses 4096 memory locations, extract the 8-bit pixels serially to perform the encryption. The encryption operation is based on XOR operation for 8-bit secret data and 8-bit key, which is easy and provides basic security to the steganography model. The 8-bit encrypted data are input to the bit mapping module which is performed based on predefined memories. Consider four-memory modules M1, M2, M3, and M4 with defined values from 0-15. Each memory is having 4 locations with 8-bits in a 2x2 matrix format. The encrypted 8-bit data is divided into four parts as E [7:6], E [5:4], E [3:2] and E [1:0], each of 2-bit size and Mapped into one of the four Memory locations of Memory modules M1, M2, M3, M4 respectively. The mapping into one of the Memory location is based on whether encrypted 2 bits are 00, 01, 10 or 11 and generate mapped data of 4-bit size as b1, b2, b3, and b4 respectively from M1, M2, M3 and M4. The Embedded module receives the serially the High pass components as an 8-bit input along with four b1, b2, b3, and b4 mapped data. Four high pass components are taken one by one and their LSB 4-bits are replaced with b1, b2, b3 and b4 respectively one by one and then the cycle repeats and operation continues till the last high pass component. The inverse –DWT is a reverse process of DWT operation. The DWT output (l) as one of the input to Inverse DWT module as an even data, which performs the inverse scaling operation and other input from the embedded module (em) as odd data which performs the scaling operation. I have followed by updating with the delta coefficient and then prediction with the gamma coefficient. The updation and prediction will be followed with other filter coefficients beta and alpha, respectively. The final high pass (ih) and low-pass components are obtained to generate the 128x128 stegano image. The recovered module consists of splitting with Lifting based DWT, pixel extraction, and bit retrieval to retrieve mapped encrypted bits using LSB method and finally decryption Module. The Recovered module hardware architecture is represented in Fig. 3.

The splitting module receives the stegano image data bits serially. After splitting, 8-bit even and odd data are generated. Perform the DWT Operation using even and odd data to generate low and high pass components. The operation of Splitting and lifting based DWT is the same as in the stegano module.

Consider the series of high-pass component to extract the pixels. The high-pass components are shifting serially one after other and use the first four high-pass components initially. Extract the 4-bit LSB data from the four high-pass components and store it as 4-bit p1, p2, p3, and p4. Perform the bit retrievals to extract the bits. Consider 4-bit p1, divide into 2-bit each, and perform XOR operation to generate the 2-bit data. Retrieve the same for other extracted bits like p2, p3, and p4 to generate 2-bit data for each. Finally, concatenate all the retrieved four 2-bits each other to form 8-bits and fed to the decryption module. Perform the XOR operation with the same 8-bit key to generate the recovered secret image. The next section evaluates the results and performance analysis of the proposed work.

V. RESULTS AND PERFORMANCE ANALYSIS

The proposed steganography model is designed using Verilog-HDL on Xilinx –ISE environment and implemented on Artix-7 FPGA. The simulation is performed using Modelsim 6.5c. The steganography model includes stegano and recovery module, and its resource constraints are tabulated in Table I. The area utilization in terms of Slice registers, Slice LUT’s, and LUT-FF pairs are noted after synthesis of Stegano and recover modules. The timing utilization includes the minimum period (ns), and maximum operating frequency is tabulated for both the modules. Along with Power utilization is performed after the place and route operation using Xilinx X-power analyzer.
The Graphical view of proposed design Synthesis results is represented in Fig. 4.

The stegano module utilizes 1272 slice LUT’s because of DWT and IDWT operations, whereas the recover module utilizes 435 slice LUT’s. The stegano and recover Module utilizes the 352 and 182 Slice Registers and 179 and 69 LUT-FF Pairs, respectively. The Maximum frequency of the stegano and recover module uses 127.915 MHz and 124.454MHz using Artix-7 FPGA device. The stegano module is operating faster than the recover Module, because of the parallel execution of bit mapping and embedding module using modified LSB technique. The stegano and recover module consume the total Power of 0.128W and 0.097W and also dynamic power of 0.046W and 0.014W, respectively.

The performance evaluation of the Steganography module is analyzed using PSNR and MSE for a different cover, and secret images are tabulated in Table II. These performance parameters are defined as

\[
MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [f(i,j) - f'(i,j)]^2
\]

\[
PSNR = 10 \log_{10} \frac{255^2 MN}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [f(i,j) - f'(i,j)]^2}
\]

The Steganography module, hardware results for different Images is represented in Fig. 5. The cover image has 128x128 image size in Fig. 5(a), the secret image is 64x64 image size in Fig. 5(b), apply the stegano module to generate the stegano image in Fig. 5(c). Also, apply the recovery module to recover the secret image in Fig. 5(d).

The different combination of different images for the cover and secret images are applied to the steganography module to analyze the performance. The Peppers + Lena as a cover and secret image gives the best PSNR of 29.0583dB and MSE ratio 326.3797. If the size of the cover images is increased, then the PSNR will be increased, and the MSR ratio will be decreased with better image quality.

The PSNR values are obtained for 5% and 10% noise is an average of 27.832dB and 26.424dB respectively. Similarly, for MSE Values are obtained for 5% and 10% noise is an average of 404.93 and 600.42 respectively. These values in comparison with Table II values show that there is a difference of 0.550 approximately.

The PSNR and MSR is calculated by adding the 5% and 10% salt and pepper noise to the obtained stegano image for below different image combinations and are tabulated in Table III.

The previous architecture [23] uses Haar DWT approaches and obtains the PSNR values for different images which is compared with proposed approaches for the same images with an improvements and are tabulated in Table IV.
The hardware architecture of previous approaches [24-25] uses Lifting based –DWT approaches on Spartan 3-EDK Processor, which consumes more chip area and operating frequency than the proposed method. Similarly, The Haar based –DWT approaches [22] using Spartan-6 FPGA device is compared with proposed method on the same FPGA device with chip area utilization improvement in Table V.

The proposed method of steganography is better compared to existing techniques for the following reasons:

- The hacker can’t be reached to secret information as a two stage encryption is used.
- A 2 dimension LDWT is converted to 1 dimension LDWT.
- LSBs of high pass coefficients are embedded with encrypted data.

### TABLE V. HARDWARE ARCHITECTURE RESOURCE COMPARISON WITH PREVIOUS APPROACHES

<table>
<thead>
<tr>
<th>Resources</th>
<th>Previous [22]</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technique Used</td>
<td>Haar-DWT +MLSB</td>
<td>Lifting-DWT +MLSB</td>
</tr>
<tr>
<td>Device</td>
<td>Spartan-6</td>
<td>Spartan-6</td>
</tr>
<tr>
<td>Slice registers</td>
<td>514</td>
<td>507</td>
</tr>
<tr>
<td>Slice FF's</td>
<td>297</td>
<td>209</td>
</tr>
<tr>
<td>4-input LUT's used</td>
<td>2108</td>
<td>1706</td>
</tr>
<tr>
<td>Max. Frequency (MHz)</td>
<td>153.312</td>
<td>100.448</td>
</tr>
</tbody>
</table>

VI. CONCLUSION AND FUTURE WORK

In this research work, an efficient steganography approach with stegano and recover modules are designed using Lifting DWT based and modified LSB method. The stegano module embedded the cover image with a secret image hiding with a simple security. The recovery module extracts and retrieves the stegano image to generate the recovered secret image with quality. The proposed work is designed and implemented on Artix-7 FPGA. The resource utilization of the stegano and recover modules in terms of area, time, and power utilization are tabulated. The steganography model works an average of maximum operation frequency with 126.5 MHz to meet the real-time requirements with high speed. The performance analysis of the steganography work is evaluated using PSNR and MSE. For different cover and secret images with an average of 28.434dB and 387.099 MSE Ratio is noticed. The result obtained with noise introduced shows that there is small variation in PSNR of about 0.550; therefore, the proposed model is robust. In future, integrate the robust security algorithm with Dual Tree Complex Wavelet Transform to the steganography model to provide better secure communication.

REFERENCES


