ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

FPGA Implementation of Vigenere Cipher Method Based on Colour Image Steganography

Mr. Mohankumar K N[1], Prof .H S Jayaramu [2], Dr. M Z Kurian[3], Dr. K B Shiva kumar[4]

M.Tech (DE), Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Prof and Head, Dept of TCE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Prof and Head, Dept of ECE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Prof, Dept of TCE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

ABSTRACT— This paper proposes a new Stenography method employing quantization table using FPGA .In this method new Vigenere Cipher is been used for encryption and decryption of the secret message. The color transformation techniques can be used to increase the modified coefficients so as to have good capacity and stego-size results.

The capacity which is the amount of information embedded in color images increases, with the number of modified quantized DWT coefficients.

KEYWORDS: Steganography, data hiding, capacity imperceptibility, stego image, FPGA, Vigenere cipher.

I. INTRODUCTION

Steganography means “covered writing” and it involves transmitting secret messages through seemingly innocuous files. The goal is not only the hiding message, also the message transmitting. There are many methods available that can hide messages in images, audio and video file. To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. Image steganography systems can be considered secure if it is impossible for attackers to detect the presence of a hidden message in the stego image by using any accessible means. Therefore, the hidden message must be invisible both perceptually and statistically in order to avoid any suspicions by the attacker. Moreover, a steganography system is perfectly secure if the statistics of the cover image and the stego image are identical. However, a steganography system fails if an attacker is able to prove the existence of a secret message or if the embedding technique arises any suspicions.

JPEG (Joint Photographic Experts Group) is the most common image format for internet and local usage as it provides large compression ratio and maintains high Image quality. Therefore, JPEG compressed images are the most suitable cover images to be used for steganography. Joint photographic expert-group (JPEG) is a famous file format for images. It applies the discrete wavelet transformer (DWT) for image content transformation. DWT is a widely used tool for frequency transformation.

II. LITERATURE SURVEY

Sunny Sachdeva and Amit Kumar [1], proposed Steganography Based on Modified Quantization Table with JPEG-JSteg where Two parameters namely Capacity and Stego-size have been compared. It has been found that capacity which is the amount of information embedding in colour images increases as the number of modified quantized DCT coefficients

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

increases. So more data can be embedding using this method as compared to JPEG-JSteg. The Stegosize also increases which is the disadvantage as compared to JPEG-JSteg in which Stego-size is small.

Nameer N. EL-Emam [2] proposed Data hiding method with High Security Using Steganography Algorithm by employing adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. This concept is based on both visual and statistical. According to the steps of design, they have concluded 16 main cases with their sub cases that cover as aspects of the input data into colour bitmap image. High security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. Their results against statistical and visual attacks are discussed and a comparison has been made with the previous Steganography algorithms like S-Tools. They have shown that there algorithm can embed efficiently a large amount of data that has been reached to 75% of the image size with high quality of the output.

Jae-Gil Yu1 [3] proposed a New Image Steganography method Based on 2k Correction and Edge- Detection which is a kind of spatial domain technique. In order to hide secret data in cover-image, they have used the just noticeable difference (JND) technique and method of contrast sensitivity function (CSF). This is an edge detection which uses a part information of each pixel-value. In order to have better imperceptibility, they proposed a mathematical method which is the 2k correction, a scheme which can embed more data than previous schemes, and shows better imperceptibility.

Neha Batra and Pooja Kaushik [4] implemented Modified Quantization Table steganographic method based on the JPEG quantization table modification. Instead of dividing cover image into 8×8 blocks, the cover image is divided into non overlapping blocks of 16×16 pixels to embed secret information. Three performance parameters namely Capacity, MSE and PSNR have been compared on different sizes of standard test images.

Implemented the proposed method and has been found that capacity which is the amount of information embedding in colour images increases as the number of modified quantized DCT coefficients increases. So more data can be embedded using of 16×16 Quantization Tables as compared to 8×8 tables. 512 × 512 pixel image has more PSNR and less MSE as compared to 256×256 pixel images. This method has better capacity of embedding message bits in image than Jsteg and Chang‘s. Since the DCT coefficients after the quantization are almost all zeros, the message capacity of Jpeg–Jsteg is very much limited. A block can embed can embed 136 × (417 × 417)/ (8 ×8) = 184757 secret bits into a cover image of 417 × 417 pixels.

Prabakaran. G and Bhavani.R [5], proposed a Digital Image Steganography method on DWT in which a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image is employed Discrete Wavelet Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego image.
T. Narasimmalou and Allen Joseph .R [6] are proposed Discrete Wavelet Transform (DWT) for transmitting pictures was proposed. Two different techniques are proposed one using three level wavelet decomposition taking a single plane of the cover image for embedding and processing the image as 4 x 4 blocks with swapping and using single level wavelet decomposition.
Septimiu Fabian Mare, and Lucian Prodan [7] was proposed high capacity steganographic algorithm based on the original smart LSB pixel mapping and data rearrangement design focusing on reducing the image degradation in the embedding process with the original luminosity of the image as a quality metric, the algorithm is capable of maintaining even more of the original color quality.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

III. PROPOSED DESIGN

A. Encryption method

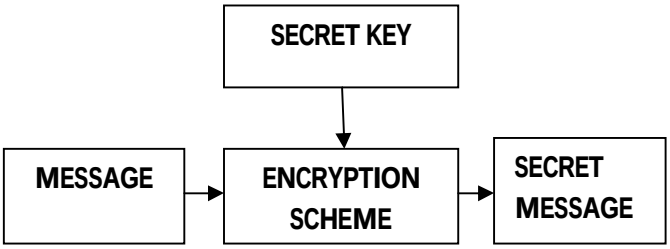

Figure 1: Encryption Block

The key: A sequence of characters.

To make brute-force decryption impractical, the key should have at least 15 or 16 characters. Also, it should not be a "special" sequence. such as an English language word. It may be best if all letters of the key are distinct.

Encryption: Duplicate the key as many times as necessary, so that the length of the (duplicated) key matches the length of the plaintext.

For i = 0, 1, 2, 3, ...:

"Add" letter i of the key to letter the i of the plaintext, to obtain letter i of the ciphertext.

(In adding letters, we identify them with integers modulo26: **a** → 0, **b** → 1, ..., **z** → 25.)
Example:
Key: **wonderland** *(10 characters, not an ideal key)*

Plaintext: **alicewasbeginningtogetverytiredof**

Key(duplicated): **wonderlandwonderlandwonderlandwon**

Ciphertext: **WZVFINLSOHCWAQMERTBJAHIHVPEIEHZCS**

We obtained letter 5 the cipher text like this:

w → 22
+ **r** → +17
N ← 13 (mod 26)

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

B. Description method

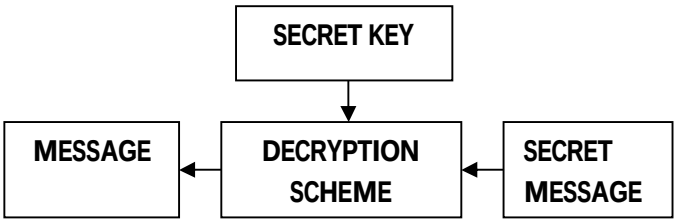

Figure 2: Decryption Block

Decryption: Like encryption, except we get the plaintext by subtracting letters of the (duplicated) key from letters of the cipher text and perform the mod (26) get the original message.

Example:

Key**: wonderlandwonderlandwonderlandwon**

Plaintext**:**
WZVFINLSOHCWAQMERTBJAHIHVPEIEHZCS

Cipher text**: alicewasbeginningtogetverytiredof**
We obtained letter 5 the *Plaintext* like this:

N → 13
- r → +17
W ← 22 (mod 26).

C. Proposed Block diagram

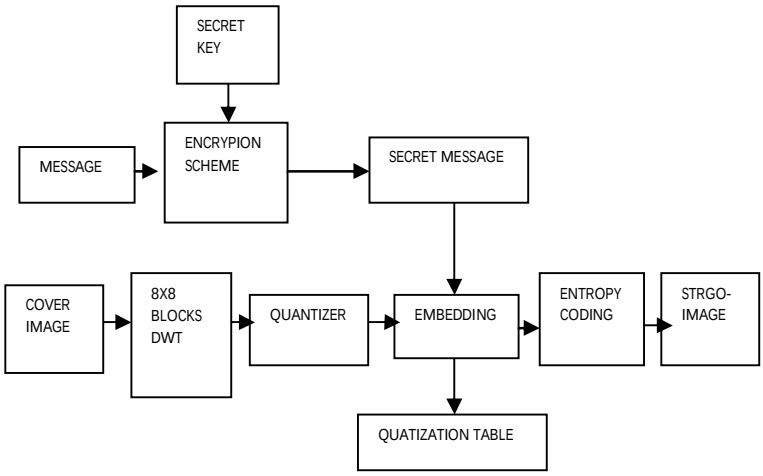

Figure 3: Embedding Procedure

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

DWT: The discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale.

Quantization is a lossy compression technique achieved by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible. For example, reducing the number of colors required to represent a digital image makes it possible to reduce its file size. Specific applications include DCT and DWT data quantization in JPEG .

Entropy encoding is a lossless data compression scheme that is independent of the specific characteristics of the medium. These entropy encoders then compress data by replacing each fixed-length input symbol with the corresponding variable-length prefix-free output codeword.

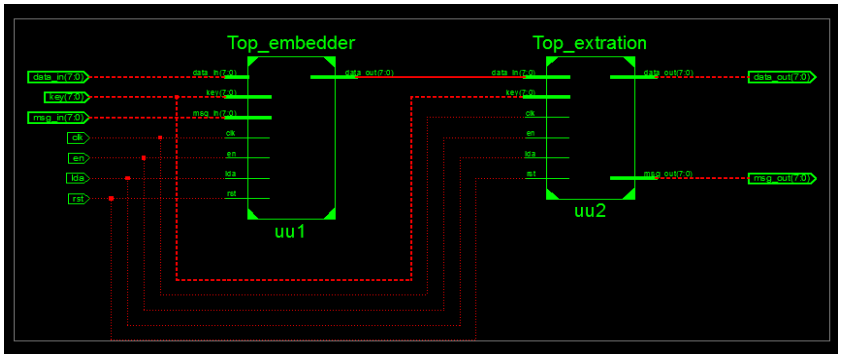

Figure 4: RTL schematic of embedding procedure

In embedding procedure, the secret message embedding into the cover image by using embedding procedure in Xilinx tool. We get stego-image.

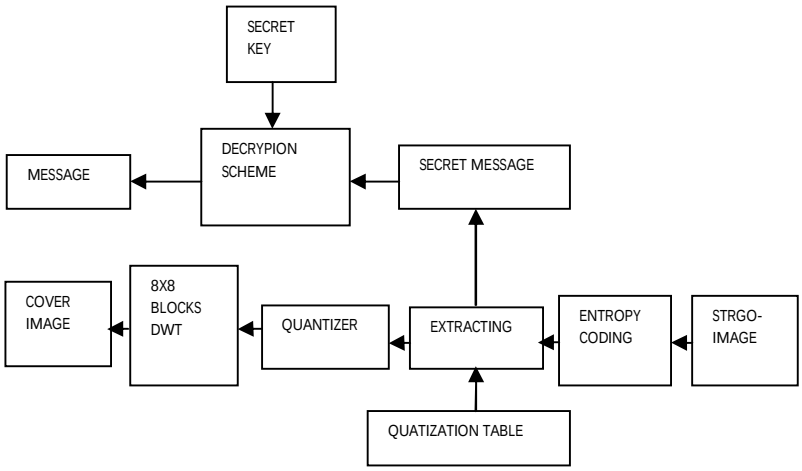

Figure 5: Extracting procedure

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

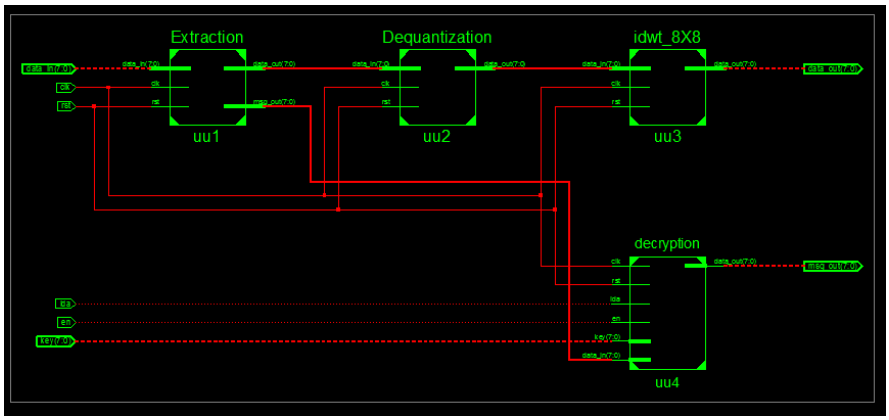

Figure 6: RTL schematic of Extracting procedure

In extracting procedure, from the received signal or image the original information is extracted by using extractor and that information is de-quantized and passed though the IDWT, this is secrete massage this is passed through the decryption block hence the original or the transmitted signal or information is recovered at the receiver.

IV. RESULTS

Encryption simulation results

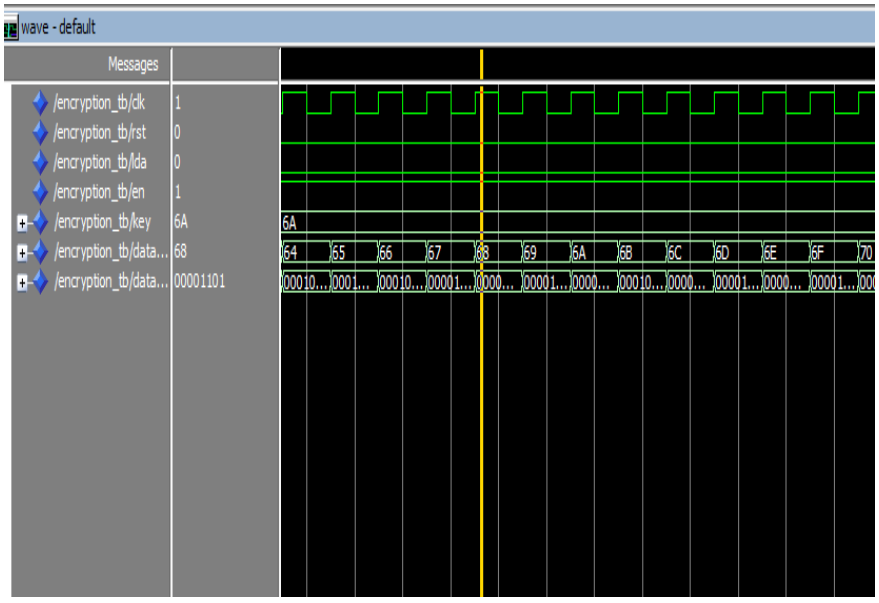

Figure 7: Encryption result

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Decryption simulation results

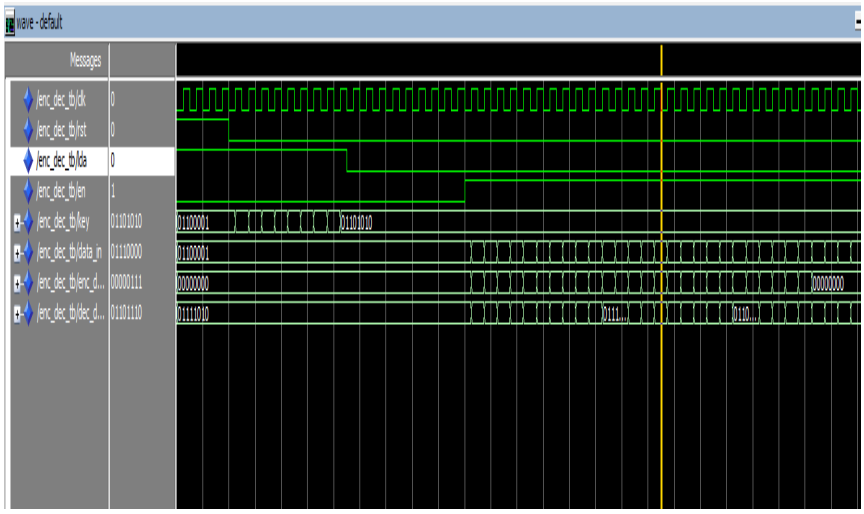

Figure8: Decryption result

In this scheme first loaded key and Cipher text and performs the decryption, if reset is one the output is zero. If make the reset is zero we get the output.

V. CONCLUSIONS

The Colour Image Steganography based on Modified Quantization Table is proposed using a new Vigenere cipher method for encryption and decryption of the secret message. In this the color transformation techniques has been used to increase the modified DWT coefficients so as to have good capacity and stego-size results and increase the message capacity embedding in the cover image using on FPGA design and implementation.

REFERENCES

[1]. Sunny Sachdeva and Amit Kumar "Colour Image Steganography Based on Modified Quantization Table", Second International Conference on Advanced Computing & Communication Technologies ,computer society,7/12/ 2012 .
[2]. N. N. EL-Emam "Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm," International Journal of Information and Communication Engineering ,4:2 :2008.
[3].J.G.Yu1, E.J.Yoon2, S.H. Shin1 and K.Y. Yoo, "A New Image Steganography Based on 2k Correction and Edge-Detection", Fifth International Conference on Information Technology: New Generations978-0-7695-3099-4/08, April 2008.
[4].Neha Batra and Pooja Kaushik implemented Modified 16×16 Quantization Table Steganography on Colour Images, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[5]. Prabakaran. G and Bhavani.R A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform, International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012.
[6].T. Narasimmalou and Allen Joseph .R Discrete Wavelet Transform Based Steganography for Transmitting Images, IEEE-International Conference On Advances In Engineering, Science And Management (lCAESM -2012) March 30, 31, 2012.
[7]. Septimiu Fabian Mare, and Lucian Prodan High capacity steganographic algorithm based on payload adaptation and optimization, 7th IEEE International Symposium on Applied Computational Intelligence and Informatics· May 24-26, 2012.