International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 7 Ver IV || July 2018 || PP 74-81

Hybrid Steganography System Using Interpolation andLSB

Savita D Torvi [1], K B ShivaKumar[2]
[1]*Research Scholar, Sri Siddhartha Academy of Higher Education, Maralur, Tumakuru, India*
[2]*Professor and HOD, Department of Telecommunication Engg., Sri Siddhartha Academy of Higher Education*
Corresponding Author:Savita D Torvi

Abstract : *Steganography is à technique of hiding data or information in the communication media which can be an audio, video, image or text file. There are different steganographic real time applications such as medical imaging, finger print and data communication in military. In this paper, a new steganographic system for real time application using digital image hiding the text has been proposed. The error pixels of the image are obtained using original pixel as well as the calculated interpolated values. The text message is encrypted and hidden into the error pixel using additive interpolation technique. Later it is implemented on FPGA and simulated using Xilinx simulator. Various parameters such as power, area, speed, throughput and efficiency are much improved compared to the existing techniques and also from the experimental results it is observed that the proposed work is more resist against the attacks.*
Keywords -*FPGA, interpolation, linear, steganography.*

Date of Submission: 09-07-2018 Date of acceptance: 23-07-2018

I. INTRODUCTION

In the recent technology computer and cyberspace are the main sources for communication, which links the distinct parts of world as one universal worldwide. In the rapid development of internet, data transmission over internet becomes the significant challenge and to protect the data while transmitting. This can be achieved by the method Steganography. As a result, the information can be transferred for longer distance, because this has the major issue to secure the information for a longer distance. This is very essential in case of transferring confidential data. This problem can be eliminated by the use of steganography methods. This steganography is powerful method and when it is combined with encryption it gives more security. The letter "Steganography" has two words stegno and graphia. Stegano means covered and graphia means writing, which means covered writing. It is come from Greek word. It is a data hiding method, which is used to transmit a message on a communication media where some other type of information is already being transmitted. The aim of Steganography is to hide information inside audio, video the text or images in such a way that the hackers should not detect the secret message present inside the cover file. Steganography attempts to hide the existence of communication.

1.1 Interpolation Error:[8]

Interpolation lie between two known valuesand interpolation values are calculated using interpolator. Linear interpolation error is the process of finding unknown values and interpolation errors obtained using the formula

$e = x - x'$ (1)

Where X is the prime pixel

X^1 is the interpolated values

The two maximum values of interpolation-error histogram are

$MaxL = \arg_{e \varepsilon E} \max hist(e)$ (2)

$Max_R = \arg_{e \varepsilon E-LM} \max hist(e)$ (3)

Where hist (e) is the number of frequency of interpolation error e**.**E is the available interpolation-errors.Then interpolation-errors are separated in two regions.

Left interpolation-errors $LE = e$ satisfies $e \le MaxL$

Right interpolation-errors $RE = e$ satisfies $e \ge Max_R$

After obtaining LE and RE hide the data in the pixel using additive interpolation error expansion using equation.

$$e(i) = \begin{cases} e(k) - sign(e) * b(k) & \text{if } e(k) \le Max_L \\ e(k) + \text{sgn}(e) * b(k) & \text{if } e(k) \ge Max_R \\ e(k) & Max_R \le e(k) \le Max_L \end{cases} \quad (4)$$

Where e^1 is the additive interpolation-error expansion, b is the embedded bit, and sign (.) is a signum function.

$$sign(e) = \begin{bmatrix} 1 & e\ \varepsilon LE \\ -1 & e\ \varepsilon RE \end{bmatrix} \quad (5)$$

To squeeze out the embedded message from the stego image, interpolation values are takenout for stego image using interpolation algorithm, the same algorithm used in the embedding process and the corresponding interpolation errors are calculated for the stego imagei.e. $e' = x'' - x'$

X'' is the stego image

X' is interpolated value

e' Is interpolation error

After that the hidden data can be removed using

$b(k) = e(i) - e'(i)$ for $e'(i) \le Max_L \parallel e'(i) \ge Max_R$ (6)

Then decrypt message XOR with a key

The original interpolation errors can be obtained using

$$e(k) = \begin{cases} e'(i) + sign(e) * b(k) & \text{if } e'(i) \le Max_L \\ e'(i) - \text{sgn}(e) * b(k) & \text{if } e'(i) \ge Max_R \\ e'(i) & Max_R \le e'(i) \le Max_L \end{cases} \quad (7)$$

The original image recovered using $X = X' + e(k)$ (8)

II. RELATED WORK

Williams Antoniopantajalaces [1] presented digital image low complexity steganographic system. In this work text data is hidden into the image file using LSB method .before embedding the image is pre-processed that is compressed the image into dynamic range and formulated interpolation errors. The encrypted text message hidden into interpolation errors using keys LM and RM.LM and RM are the first maximum value of frequency of occurrence of hist(e), after embedding the data and implemented on FPGA of vertex 4,vertex 5 and vertex 6 and simulated on Xilinx simulator and analysed the parameter area, power, speed throughput and efficiency. From the result explained that vertex 6 high throughput and efficiency.

M C Hanumantharaju and SathishShet [2] described the new reconfigurable hardware for LSB. This was implemented on FPGA. The proposed steganography system integrated parallel and pipelining operations and produced largest throughput. The steganography algorithms were simulated and implemented on FPGA for different embedding bit size and cover image resolution. This work implemented hiding and extraction process of LSB on FPGA and simulated using Xilinx vertex –II pro XC2V500FG256-6 device. The algorithm was simulated on MATLAB before implementing on hardware with resolution 1024x768 and maximum frequency 144.3MHz.It is also simulated on Xilinx synthesize the hardware and produced improved speed, area and power.

Bhardwaj Reddy et al., [3] emphasises that pixels are the main features of image which are used for analysing and processing the images in edge detection. The speed of operation increases when the system is implemented on FPGA for different image edge detection using Robert, pewit, sobel and laplacian of Gaussian operators using graphical user interface which combines MATLAB and XSG. Xilinx system generator is used to generate the code which is used for hardware implementation on FPGA. Among all the edge detections, laplacian of Gaussian operators has the best PSNR value with better edges.

Jose Juan Garcia-Hernandez et al., [4] described the low complexity steganographic system in spatial domain where the signature is hidden in the red component and the text message is hidden in the green as well as blue component. The proposed LSB algorithms are performed using MATLAB software and implemented using FPGA.

LixinLuo et al., [6] Proposed model stenographic system for digital images. The steganographic system used interpolation error expansion for embedding. From the result it is observed that the steganographic system has high perceptual transparency with computational complexity low and embedding rate is constant.

III. PROPOSED EMBEDDING SCHEME

The proposed embedding scheme has three stages

(a) Interpolation error b) Encryption c) Embedding

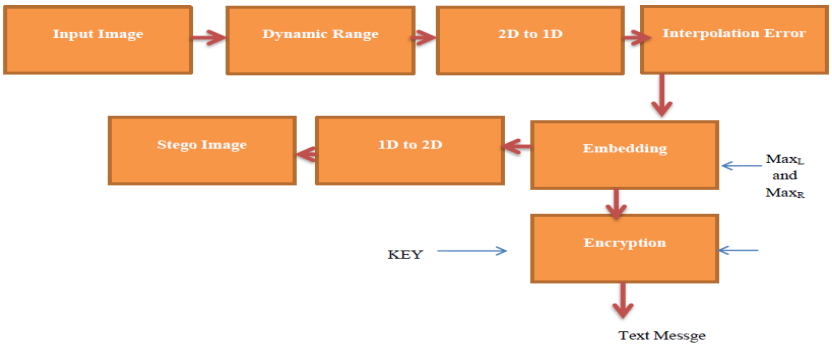


Fig1. Block diagram for embedding process

The input image [0 255] is converting into dynamic range [1 254] using round function to avoid the overflow and underflow of image and Resize the image to original size. Calculate interpolated values using interpolator and obtain the interpolation errors using original signal values(X) and interpolated values(X^1). Find the histogram errors for interpolation error. From histogram error find the two maximum occurrence of interpolation errors Max_L and Max_R using equation (2) and (3). Max_L is first highest occurrence andMax_R is the next highest occurrence of hist (e).Based upon these values fragmented interpolation errors in to two regions left interpolation errors (LE =e $\leq Max_L$) and right interpolation errors (RE = e $\geq Max_R$).

Encryption: In the encryption stage the text message is encrypted with the key using XOR. The same key is used for the decryption. The encrypted message is hidden into the error pixel.

Embedding: The text message hidden in to the images using LSB .In this stage the interpolation errors e(0),e(1)…… are checked whether the e(0) is in left interpolation error (LE)or right interpolation error(RE),according to the equation (5) embed the message bit . In this way the text messages are hidden into the images.

3.2. Extraction Process: Fig 2 shows the block diagram of extraction process. This is the inverse of embedding process calculate interpolation errors using interpolated values and original signal values, interpolation errors, linear interpolation error histogram. And embedded data can be obtained by equation (5) and (6).

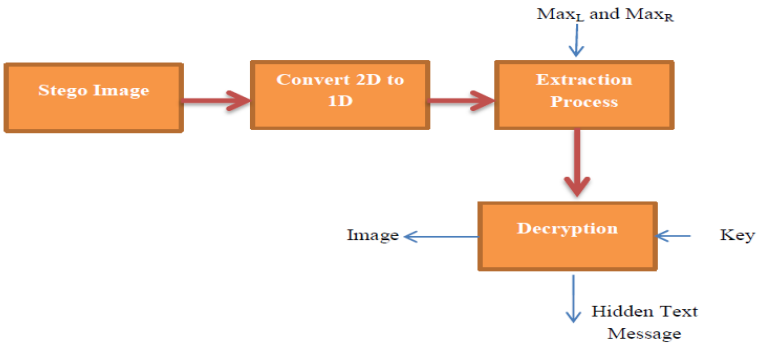


Fig2. Block diagram for Extraction process

Algorithms:

a) Embedding:

i) Read the cover image

ii) Compress the cover image into dynamic range [0 255] to [1 254] using round function

$x = \text{round}\left(253 \times \frac{\max}{255}\right) + 1$ Where 'max' is maximum intensity of cover image.

iii) Resize the image.

iv) Convert2D image to 1D.

v) Calculate interpolated values X^1using interpolator.

vi) Calculate the interpolation error using equation (1)

vii) Formulate interpolation error histogram hist (e).

viii) Obtain Max_L, Max_RUsing (2) and (3).

ix) Encrypt the text message using key

x) Embed the encrypted message in the LSB bit of interpolation error pixels using (4) and (5).

xi) Resize the stego image from 1D to 2D

b) Extraction:
i) Convert stego image from 2D to 1D.
ii) Calculate values x' for stego image using interpolator And also calculate interpolation error the same procedure used in the embedding process.
iii) Tear out the hidden bit using equation (6).
iv) Decryptextracted message with key.
v) Original interpolation error can be extracted usingequation (7)
vi) Original image removed using equation (8)

IV. RESULTS

A) 4.1 Experimental results of Area, Power and Delay:The proposed work is implemented on reconfigurable FPGA device for embedding and extraction algorithms of LSB. The FPGA family choosen are vertex4 (90nm), vertex 5(65nm) and vertex 6(45nm) .The design algorithm run in model sim simulator Xilinx 13.1 and is synthesized, place and routed, and implemented on FPGA.

Fig3. Shows top level steganography module. The top design module requests different sub-modules obtained in the form of tree structure. The design is synthesized, place and routed, and implemented on FPGA device and simulated using Xilinx simulator. From the result it is observed that the proposed algorithm take less area and speed with increasing power and also the computational complexity is reduced.

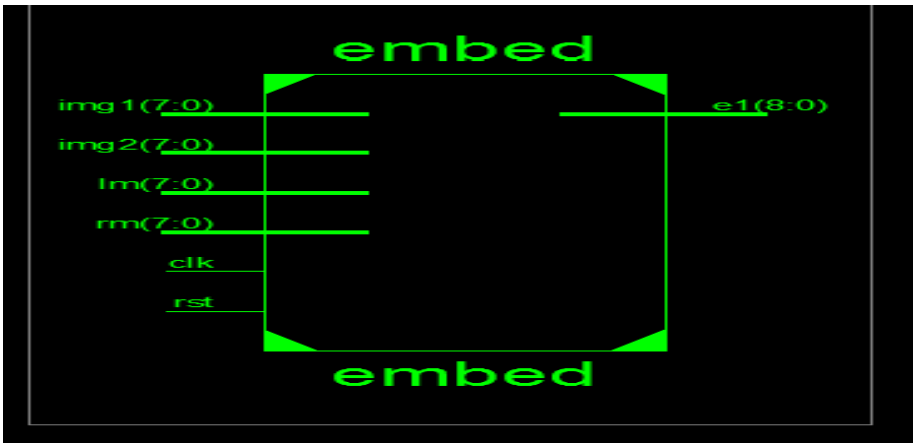


Fig3. Top module entity

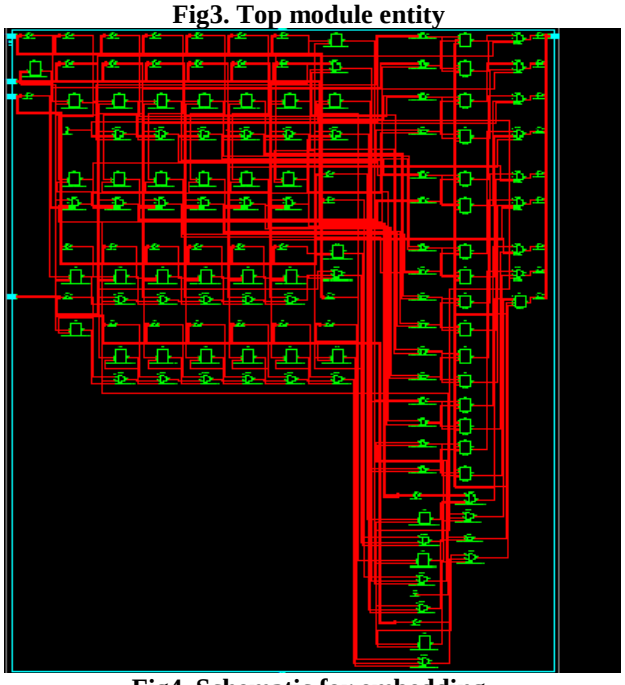


Fig4. Schematic for embedding

Table1. Data for area, delay, throughput, efficiency

Integration technology	Slice luts (area)	Delay (ns)	Frequency (MHz)	Throughput (MPPS)	Efficiency
Virtex 4 (90nm)	4760	6.775	140.6	787.36	51.8x10^3
Virtex 5 (65nm)	4784	6.704	149.16	835.2	86.35*10^3
Virtex 6 (40nm)	4827	6.544	152.8	855.68	100.42*10^3

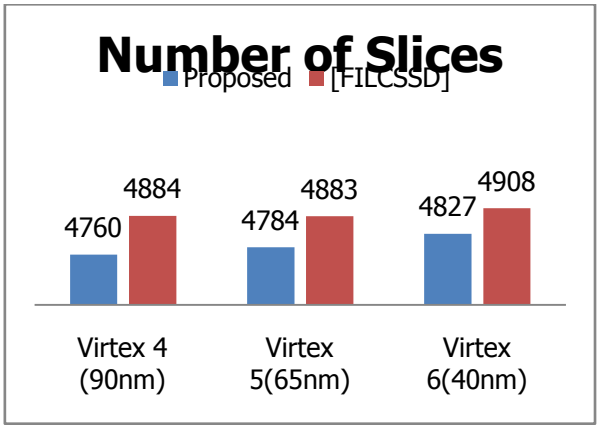
Table2. Comparison table

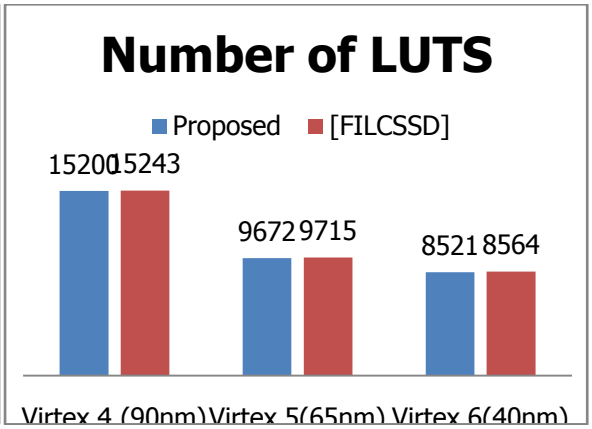
Integration technology	[FILCSSD] Slice (area)	Slice register (area)	[FILCSSD] Slice LUTs	Slice LuTS	[FILCSSD] Delay (ms)	Delay (ns)	[FILCSSD] Power (W)	Power (W)
Virtex 4 (90nm)	4884	4760	15243	15200	1.07	6.775	1.638	1.293
Virtex 5(65nm)	4883	4784	9715	9672	0.936	6.704	0.696	0.431
Virtex 6(40nm)	4908	4827	8564	8521	0.868	4.386	0.463	0.322

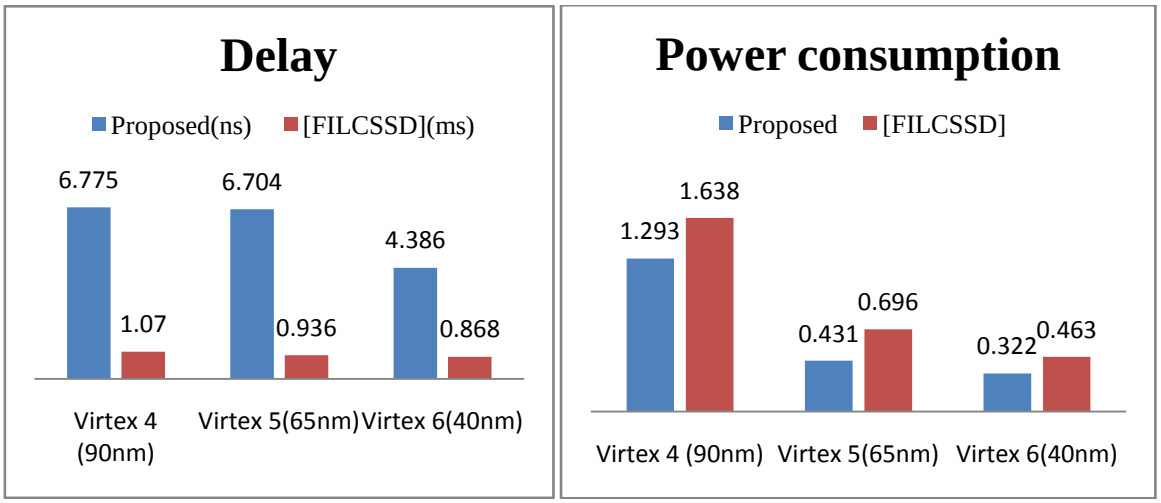
Table3. Comparison table

Frequency [MHz] [FILCSSD]	Frequency (MHz)	Throughput (MPPS) [FILCSSD]	Throughput (MPPS)	Efficiency [FILCSSD]	Efficiency
84	100.2	641.26	787.36	42.069*10^3	51.8x10^3
96	109	734.17	835.2	75.57*10^3	86.35*10^3
100	112	764.63	855.68	89.28 x 10^3	100.42*10^3

Table2 and Table3 is the comparison table with the existing technique. From the table it is observed that efficiency and throughput increased along with reduced speed, area with increasing power.







B) 4.2 Analysis for security

4.2.1 Chi-Square Attack: Westfeld and Pfitzmann [2] explained the detection of data in LSB embedding digital images.

Chi-square steganalysis: The Chi-square assault is one of the methods to investigate the detection of any hidden statistics. This takes a test and depending on the density with which pixel intensity appear. The Chi-squared attack was designed to detect this near-equal basis. The probability of embedding is approximately is equal to zero when ξ^2_{n-1} value high. The probability of embedding is 1 when ξ^2_{n-1} value is less. Therefore the ξ^2_{n-1} value is approximately is equal to 1.

LSB technique hides the information in the LSB of the image intensity. If the original bit is differing from the hidden bit then bit manipulation must be used.

Let i is the pixel intensity, i Є $(0, 2^8)$.

Ifi=2j then after manipulation i will be 2j+1 and

Ifi=2j+1 then after manipulation i=2j.

$$\xi^2 = \sum_{i=0}^{N} \frac{(xi - yi)}{zi}$$

According to the pair of values (POV) concept, 2j and 2j+1 two pixels combines as a pair and they differ only in the least significant bit.

Let h_{2j} is the frequencyof 2_j pixel, h_{2j+1} the frequencyof 2_{j+1} pixel. The frequencies of the pov of two pixel values are same. The chi - square test is utilized to decide the critical distinction in the recurrence of POV. Chi-square measurements are utilized to find the frequencies of POV are the likelihood of measurement under the condition that the conveyances of x_i and y_i are equal. It is calculated by integration of the density function.

$$\xi^2_{n-1} = 1 - \frac{1}{2^{\frac{(n-1)}{2}}\Gamma\frac{(n-1)}{2}} \int_0^{\xi^2_{n-1}} e^{-\frac{u}{2}} u^{\frac{n-1}{2}-1} du$$

In the proposed work the probability density function is 1 therefore the chi-square value is zero. Hence the proposed work is more resist against the chi-square attack.

4.2.2 Image entropy: The entropy is used for measuring security for the stego image let H (1), H (2), H (n) are the possible intensity values for data hiding. Then P (H1), P (H2), P (H3) is the probabilities of getting particular intensity. Therefore the entropy of an image is calculated by the following expression.

$$Entropy = -\sum_{i=0}^{n-1} H(i) \log H_2(i)$$

The entropy of different images is calculated and is tabulated.

Table4. Entropy for different images

Images	Entropy
Onion	7.42
Baboon	7.087
Lena	7.92
Boat	7.02
Hibiscus	7.49

Information entropy of different images is as shown in table. The entropy value H (n) is approximately equal to 8that mean the leakage of information is negligible. Hence our proposed work is more resist against the attack.

4.2.3 NPCR (number of changing pixel rate): The number of pixels changing rate measures the rate of pixels changing into the stego image. It is calculated by the following equation.

$$NPCR = \frac{1}{M * N} \sum_{i,j} G(i, j)$$

$$G(i, j) = \begin{bmatrix} 1 \text{ if } G1(i,j) = G2(i,j) \\ 0 \text{ if } G1(i,j) \neq G2(i,j \end{bmatrix}$$

G1 (i,j) is the original image.

G2 (i,j) is the stego image.

4.2.4UACI: (unified average changed intensity): It finds the average intensity of the difference between stego image and original image. It is calculated by the following expression is the largest supported pixel value compatible with the stego image.

$$uaci = \frac{1}{M * N} \sum_{i,j} \frac{|G1(i, j) - G2(i.j)|}{T}$$

4.2.5 Normalised cross correlation (NCC): The normalized cross correlation is used to measure the amount of deviation in the stego image with respect to cover image after embedding the data and is calculated by the following expression.

$$NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} [X_{ij} * Y_{ij}]}{\sum_{i=1}^{N} \sum_{j=1}^{M} [X_{ij}]^2}$$

Table5. Values for different Images

Images	NPCR	UACI	NCC	SSIM
Onion	0.05	0.0412	1.195	0.99993
baboon	0.0896	0.0386	1.138	0.99995
Lena	0.055	0.0307	1.103	0.99993
Boat	0.054	0.0412	1.0625	0.95971

From the table it is observed that the NPCR value is very high as compared to the UACI and also the NCC value is 1(the ideal value is 1) in all images. Hence our proposed work is more resist against the attack.

4.2.6PSNR (peak signal to noise ratio): PSNR is another parameter is used tomeasure the quality of the sego image and it is calculated by using the formula.

$$PSNR = 10 \log_{10} \frac{255}{mse}$$

From the result it is observed that the PSNR value is improved .the graph of embedding capacity versus PSNRand MSE is as shown in fig5 and fig6. As the embedding capacity increase the PSNR value decereases and mse value increases.

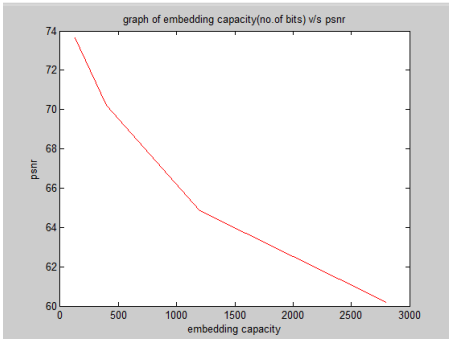


Fig5. Embedding capacity versus PSNR

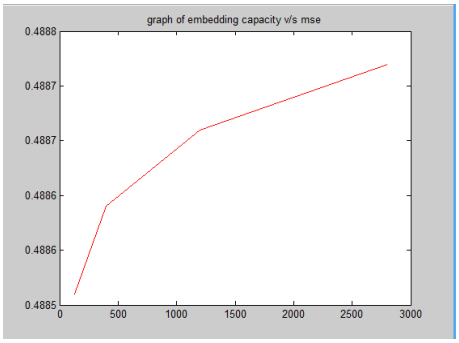


Fig6. Embedding capacity versus MSE

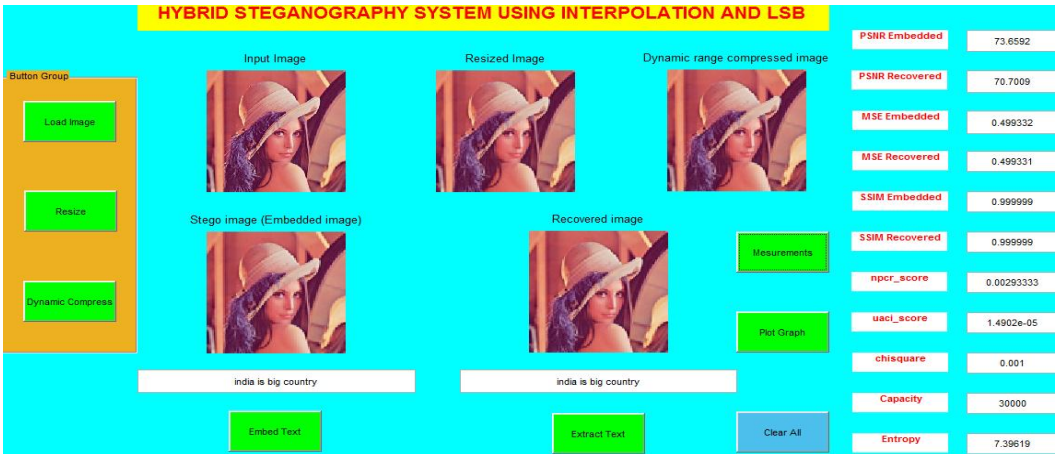


Fig7. Embedding capacity of 128 bits

V. CONCLUSION

The proposed work hides the encrypted text message in an image using LSB and is implemented on FPGA using Xilinx Virtex-4, Vertex -5 and Vertex- 6 with less delay, less area with increase in power and increase in throughput as well as efficiency. This new hardware structure can be used for real time application because it is implemented on reconfigurable device. In Future work, hardware implementation of more complex random-based LSB method may be used to improve the area, speed and power.

REFERENCES

[1]. Williams Antonio pantajalaces "FPGA implementation of low complexity steganography system for digital images". PP: 319-324, IEEE ICIS 2015.

[2]. M. C. Hanumantharaju3 & Xiao-Zhi Gao4 K. SathishShet& A. R. Aswath "Design and development of new reconfigurable architectures for lsb /multi-bit image steganography system" Multimed Tools Appl DOI 10.1007/s11042-016-3736-0 Springer.

[3]. G. Bhardwaj Reddy "content – implementation of image edge detection on FPGA using XSG". PP: 1-5, IEEE 2016[ICCPCT].

[4]. Jose Juan Garcia-Hernandez "on a low complexity steganographic system for digital images based on interpolation error expansion" pp. 1375-1378, IEEE 2013

[5]. E.A.Elshazly, Safey A.,R.M.Fikry , S.M., O.Zahran, M.El-Kordy "content – FPGA implementation of robust image steganography technique based on least significant bi(LSB) in special domain" IJCA, vol.145, PP:43-52, JULY 2016.

[6]. LixinLuo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong "content – reversible watermarking using interpolation technique" IEEE Transaction on Information forensics and security, vol.5, no.1, PP: 187-193, March

Savita D Torvi "Hybrid Steganography System Using Interpolation and LSB "International Journal of Engineering Science Invention (IJESI), vol. 07, no. 07, 2018, pp74-81