DWT Based Image Steganography with Seven Segment Display Pattern as a Key

Savita D Torvi, K B Shiva Kumar

Abstract*: *Steganography is one of the commanding and commonly used methods for embedding data. Realizing steganography in hardware supports to speed up steganography. This work realizesthe novel approach for generation of Key, for hiding and encoding processes of image steganography using LSB and HAAR DWT.The data embedding process is realized with seven segment display pattern as a secret key with various sizes using HAAR DWT and LSB. Maximum hiding effectiveness is also attained from this work. The same is implemented in hardware using reconfigurable device Field programmable gate array to improve the speed, area and power. The proposed work is also evaluated improved PSNR using MATLAB.

Index Terms*: *Seven Segment Display, Steganography, Least Significant Bit (LSB), FPGA, DWT.

.

I. INTRODUCTION

In the present days, communication can be completed between two or more individualexistence at different residences through internet. For trusted communication, i.e., the interactive message is not exposed; the message must be scrambled before transfer. If the confidential message is perceived by an attacker, it may be susceptible. The clarification of such sorts of difficulties is delivered by steganography. The term 'steganography' is the amalgamation of two Greek words "stegano" and "graphia" which means covered and writing .In fact, there are three major divisions of data hiding namely DigitalWatermarking, Cryptography andSteganography.

A digital image is a two dimensional matrix of the intensity values onevery grid point. Gray images contain eight bits, whereasRGB images usetwenty four bits to designate the color model. Generallyembedding is done either in Time domain or Frequency domain or in both.

The time domain implants stealthy statistics in the lowermost bit of image pixel. The least significant bit method is easy for implementation. However,it is delicate in contrast tolimitedassaultswhereas the frequency domain hides the secured information in the image frequency constants, which decreases the problems,originate in the time domain.

Steganalysis is the technique of recognizingcovered evidence which is created using steganography.Steganalysis treasures stego images of investigativenumerous image structuresamong cover-image and stego-images.

In recent Technology,Field programmable gate array hardware is designed for emerging numerous steganography methods. If the informationimplanting function isperformed by the Field Programmable Gate Array (FPGA) integrated circuit, the execution speed is high and the optimization in resource utilization and power consumptionbecause of customized integrated circuit .The Field programmable gate array groundedinformationembedding is used as a real time implementation

II. STEGANOGRAPHY PARAMETERS:

Mean Square Error (MSE): This evaluation is achieved on the stego image and cover-image.

mse = $(1/m*n)\ \Sigma\ \Sigma\ (fij - gij)^2$

Thenumber of width is m, andthe number of height is n of thecarrier media.

fij is the intensity of carrier image ,gij is the intensity of stego media. TheGreater MSE range displays deviance among cover and stego images.

Peak Signal-to-Noise Ratio (PSNR): "Peak signal-to-noise ratio calculates the excellence of the stego-image equated with the cover image". It is calculated using the equation in db.

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

In the following, the important terms used in the proposed technique are briefly defined first, then the algorithms used for embedding and extraction processes are described. Seven segment display pattern is used as key for the embedding and extraction, this seven segment pattern is generated by using multimedia file as presented in Fig.1 and Fig.2 [1]

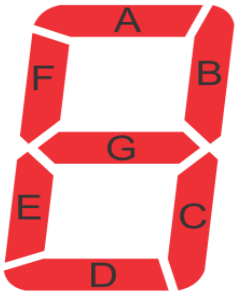


Fig .1 Seven segment display

Revised Manuscript Received on July 08, 2019.

Savita D Torvi, Research Scholar, Sri Siddhartha Academy of Higher Education, Maralur, Tumakuru, India. bitmist2017@gmail.com

K B ShivaKumar, Professor and HOD, Department of Telecommunication Engg. Sri Siddhartha Academy of Higher Education.

pattern

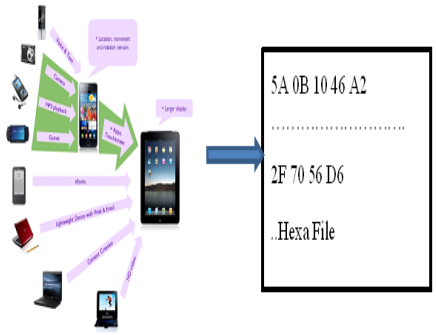


Fig .2 Multimedia file

III. RELATED WORK:

Mohammed Abbas Fadhil Al-Husainy [1] presented novel method for key generation for embedding-decoding procedures of steganography system image is as the carrier file. Thearbitrariness of safetykey is essential for hidingprocedure is attained with the seven segment display designs with various dimensions. High payload hiding effectiveness is accomplished. The proposed work improved the psnr and mse values.

Nikhil Simha H.N.et al., [2] presented an image Steganography system with DWT and Modified LSB method. It uses DWT to find low frequency and high frequency components. The Image Steganographic procedure is applied to LL band. The inverse LSB procedure was used in the decryption. The same work is implemented on FPGA. Memory prerequisite of the proposal is a smaller amount for hardware implementation. The projected method obtained improved PSNR operating frequency.

Abdullah AlWatyan et al.,[3] discussed a two stage security arrangement. In the first stage encrypt the message bits then concealed the information in cover image. The process of encryption and hiding takes 1-1-0 LSB technique. The proposed work is implemented on FPGA that yields a reduction in area and improved PSNR.

Hamad A. A. et al., [4] suggested a maximum embedding capacity and effective steganography system, where binary, RGB images, and huge script documents are hidden into a single carrier file using HAAR DWT.

Chao wang et al., [5] presenteda fast matrix hiding procedure. The proposed technique usesmatrix extendingprocedure for decreasing the computational complexity.

Vasantha and Vidhyaa [6] discussed hardware implemented steganographic system. The proposed work realized on Spartan-6 FPGA and synthesized using VHDL code. Thehardware consumption is very less related to existing methods since of simple architecture.

Ran-Zan and Yeh-Shun [7] suggested Steganography system using two ways block matching method. This system first produces anorder of blocks and at that time it searches theanalogous blocks in the carrier file. Hop implanting arrangements are used to embed information into carrier image. Thissystemprovidingimproved PSNR.

Mohd B.J et al., [8] discussed a steganography system with the least significant bit method on Field programmable gate array hardware. The Field programmable gate arrays receive the carrier image and pay load information, placed on the least significant bitscheme and yields the stegoimage. This work used an n bit least significant bitmethod that permits the user to select number of stealthy information bits embed in the individualintensity. The amount of bits is extended from one to eight bits per component. From the result it is observed that the PSNR value is increased.

Shweta Modi and Meghana Kulkarni [9] explained steganography systemusing DWT and average LSB method. The DWT-IDWT is used to familiarize randomness of the pixel values existing inside cover image. The absolute block is used to force negative coefficient values to zero, which increase the PSNR values of the rebuilt Image. The average alpha blending system decreases the bit size of the communicated stegano image as a result low communication channel bandwidth is essential to communicate the stego image. The proposed method can be capable to deliver good accuracy of hidden images and cover image in-terms of great PSNR values than present practices due to above explanations. Also the presented system uses 7% less hardware capitals than current methods and the operating frequency is 50% higher than present methods. This is because the proposed architecture is constructed using basic logic gates; no multiplier is being used.

Mahmoud pour and Mirzakuchaki [10] Discussed hardware implementation of n-bit least significant bit algorithm and Also, randomization approaches and Zhange's Least significant bit procedure were used to increase the security of least significant bit algorithm .The security is enhanced by means of a message bit randomizer to create it tougher for the assailants to form the concealed information without a safety key. Also, the extra security used to the least significant technique with the pixel interleaves method.

Maya and Sabarinath [11] presented a novel steganography system with least significant bit and DWT technique to embed information in one or more file. This system produced improved speed, which generates it very valuable for existing applications. But, the proposed used 8-bit gray scale images for concealing the data.

Patel.H and P. Dave [12] discussed a discrete cosine transform technique used to divide the carrier image into three frequency components. These frequency components arehigh, middle and low. This method uses the constants of the carrier file to conceal the pay load image using least significant bit while neglecting optical degradation. This system needs keys that must be recognized by the transmitter and the receiver.

Nikita Sharma and Meha Khera [13] presented two combined steganography approaches to get secured communication among transmitter and receiver. The proposed work used HASH LSB technique for embedding and RSA cryptography method for encoding. Before embedding the author used DWT for cover image then, encrypted message is concealed into the LL, HH band of spectrum, which improves the embedding capacity and PSNR.

Bassam et al., [14] developed hardware implementation of steganography with least significant bit using FPGA. The projectedalgorithm uses n-bit for embedding. From theresult it is observed that the improved Peak to signal ratio of two bit and three bitleast significant bit for different images.

IV. PROPOSED BLOCK DIAGRAM:

Embedding:

This proposed workis an image steganography method of full embeding capacity. This is completed through the use of the seven segment display pattern, shown in Fig.1 accomplishing randomness in the choice of bytes for hiding the secret message bits. The payload image is reflected as a collection of bytes and each byte signifies two hexadecimal digits.There are two phases in embedding.

i) Apply DWTto cover image

ii) Generation of Key using seven segment Pattern.

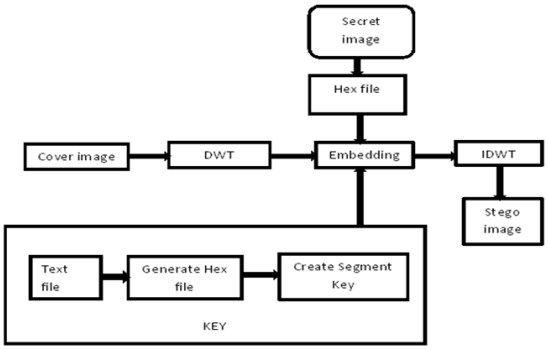


Fig .3 Embedding block diagram

Embedding Algorithm:

- Read the secret image (SI)
- Rearrange the bytes in the secret image randomly.
- Convert all the bytes in the secret image into binary stream.
- Store all the bits in 1D form.
- Group the binary stream into 8 bits to form byte and then convert all the bytes into hexadecimal number.
- Read secret key text file, convert into hexadecimal and split into Most Significant Digit (MSD) and the Least Significant Digit (LSD)
- Based on segment length create a table which has number of segments used and number of bytes used for each hexa decimal digit when it is represented as seven segment pattern.
- Read the Cover image
- Apply HAAR DWT for cover image.
- Select LL, LH, HL and HH band for embedding the message bits.
- Segment the band spectrums into segments, based on segment length.

Assume segment length=2

A 2D matrix of size is calculated by (((SL×2) +3) × (SL+2)).

((SL×2) +3) is the number of rows and (SL+2) is the number of columns of seven segment display pattern

Segment length=2

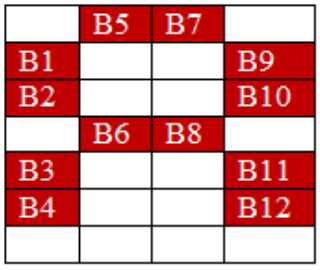
Matrix size is 7 x4

Divide the spectrum into 7x4segments

- Read the segment from the carrier image and embed secrete bits in the cells of seven segment pattern in column by column as shown in fig
- Embed the secrete message bits in the lsb of seven segment display pattern of the cover image.

For example if the secret key A0B8…

B0	B2	B3	B4	B5	B6	B7	B8
1	0	1	0	0	0	0	0

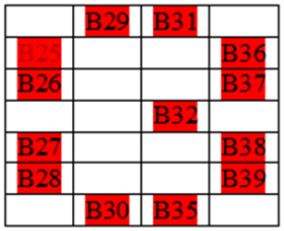


(a)

B9	B10	B11	B12	B13	B14	B15	B16
0	0	0	0	0	0	0	0

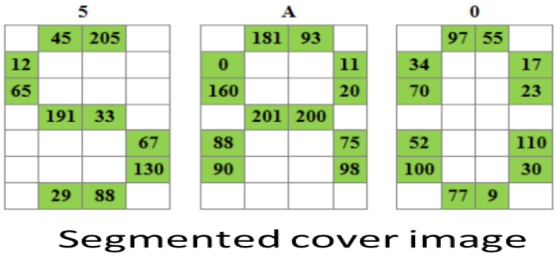
(b)

B17	B18	B19	B20	B21	B22	B23	B24
1	0	1	1	1	0	0	0

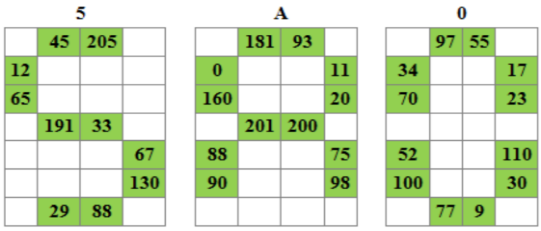


(c)

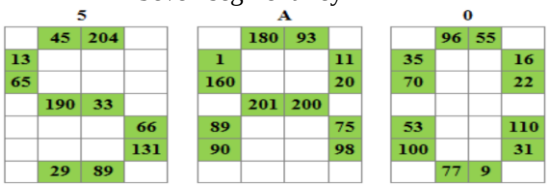
Fig.4 seven segment pattern and bit Pattern for “A”,”0”and “B”



Segmented cover image



Seven segment key



Embedded Data

V. EXTRACTION PROCESS:

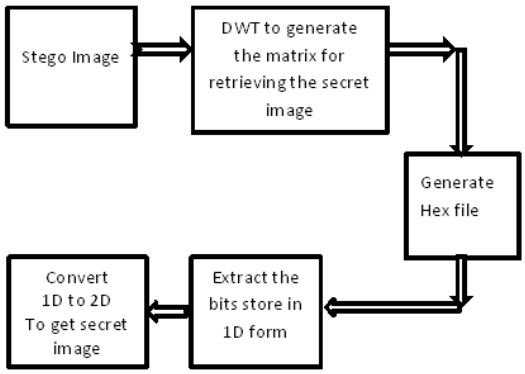


Fig.5 Extraction block diagram

VI. EXTRACTION ALGORITHM:

To extract the embedding bits in the stego image, the following steps are used

- Perform the same procedure done in step1to step6as in embedding process.
- If there are more bytes in the stego image segment, read a set of bytes from segment that are enough to fill the cells of the desired segments sequentially in the seven-segment pattern.
- Scan the segment pattern in display in the seven segment pattern.
- Remove the bits in the LSB of the bytes in the cells of the segments according to the sequence of each cell in the seven segment display pattern.

If the Byte is even, then the Bit = 0

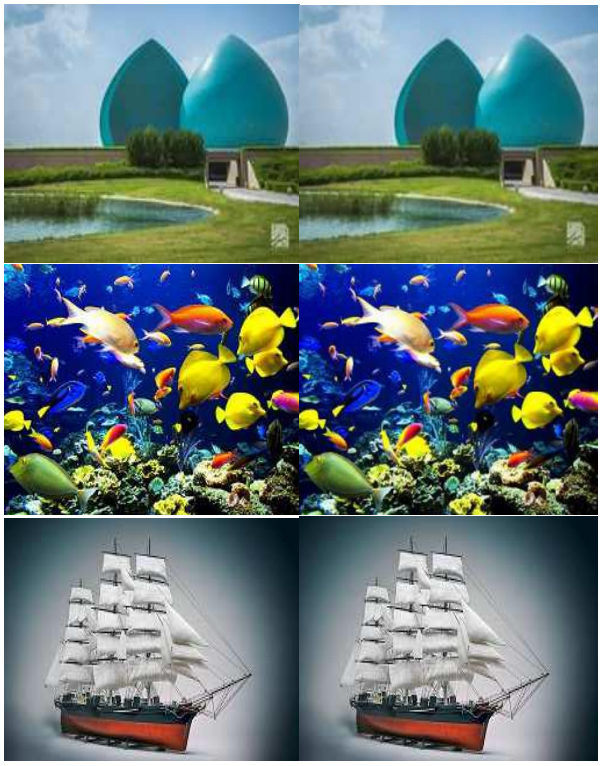
If the Byte is odd, then the Bit = 1

- Reshuffle the bits of the secret message as a one-dimensional array of bytes by renovating all 8-bits to its equivalent byte.
- Convert 1D to 2D to get secret message.

VII. RESULT ANALYSIS:

This unit gives the hardware implementation results using field programmable Gate Array for embedding information using seven segment display pattern is used as a key. Various carrier and stego images are as shown in Fig.2 and Fig.3.Then the information concealing approach is exhibited as a Verilog HDL top level entity and is simulated with Xilinx ISE 13.2. This approach used XC6VCX75t device of virtex 6 family and package of 2ff484. The resource utilization summary for the information embedding approach is shown in the Table 2.

From Table.2 and Table.3, it is perceived that the proposed work takes less time and small amount of resource utilization for realizing this algorithm and also it has the high embedding capacity of 1,51,296 bits with a high PSNR of 54.34db.



(c) Fig.6 Cover images and Stego images

Table.1 processingtime for different segment length

Images	SL	PSNR (DB)	Processing Time (nsec)
Edifice	2	54.34	6.348
Fish	20	54.42	6.358
Ship	100	54.86	6.548

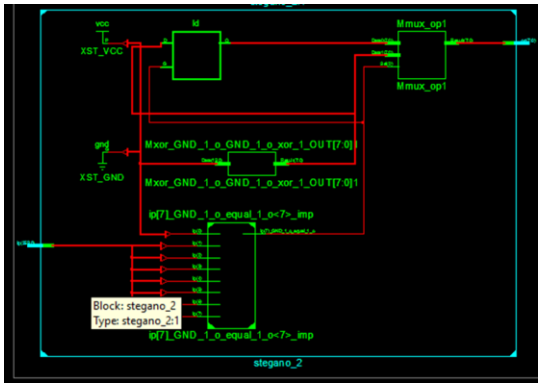


Fig.7embedding RTL schematic

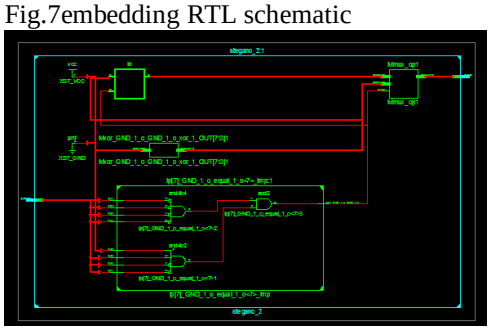


Fig.8 RTL Embedding schematic

Extraction process:

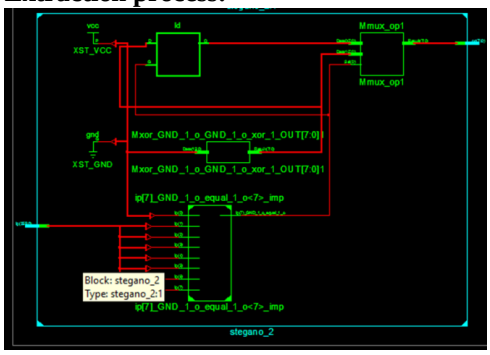


Fig.9 Extraction RTL schematic

Table 2 Resource utilization

Parameters	Experimental Results
Area	224
Speed	6.348ns
Power	1.293w

Parameters	Quantity
No. of slice register	1
No. of slice LUTs	2
No. of occupied slices	7
No. of occupied IOBs	17

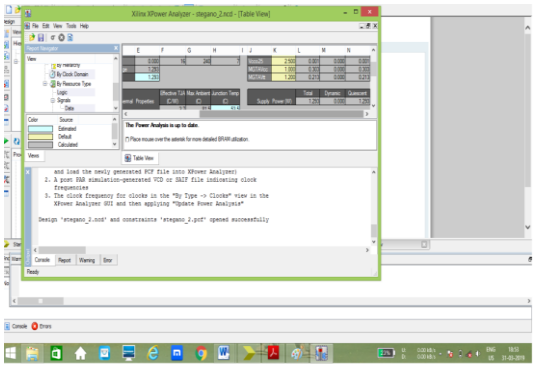


Fig.10 Power report

Security Analysis:

In this section the proposed work test the resistance of the security.

Image entropy:

The entropy is used for computing security for the stego image let H (1), H (2), H (n) are the possible intensity values for data hiding. Then K (H1).K (H2), K (H3) is the probabilities of getting particular intensity. Hence the entropy of an image is calculated by the equation.

$$Entropy = -\sum_{i=0}^{n-1} p(i)\log_2 p(i)$$

The entropy of various images is estimated and is tabulated.

Number of changing pixel rate (NPCR):

It is the measure of rate of changing pixels in the stego image. It is estimated by the following expression. K1 (i, j) is the original image. K2 (i, j) is the stego image.

$$NPCR = \frac{1}{m*n}\sum_{i,j} K(i,j)$$

$$H(i,j) = \begin{bmatrix} 1 \text{ if } k1(i,j) = k2(i,j) \\ 0 \text{ if } k1(i,j) \neq k2(i,j) \end{bmatrix}$$

Unified average changed intensity (UACI):

It computes the average intensity of the changein stego and cover image. It is designed with the equation.

$$UACI = \frac{1}{M*N}\sum \frac{|H1(i,j) - H_2(i,j)|}{T}$$

Normalised cross correlation (NCC):

The standardized cross correlation is the measure of the quantity of deviance in the stego media with respect to cover media and is designed by the equation.

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

Form the Table.3it 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 and Information entropy of different images is as shown in table. The entropy value H (n) is approximately equal to 8.that means the leakage of information is minor. Hence the proposed work is more fight back against the attack.

Table.3 NPCR, UACI, NCC, SSIM and ENTROPY values for different images

Images	*NPCR*	*UACI*	*NCC*	*SSIM*	*ENTROPY*
Edifice	0.06	0.0422	1.197	0.99997	7.926
Fish	0.0796	0.0486	1.128	0.99992	7.942
Ship	0.0556	0.0317	1.113	0.99996	7.821

Comparison of proposed model with existing work:

Table 4 comparison the proposed work with Existing work

	Nikhil Simha[2]	Proposed Work

No. of fully used LUT-FF pairs	**514**	**224**
Maximum operating frequency(MHZ)	**153.312**	**157.86**
Power in watts	**1.634**	**1.293**
Embedding Capacity	**65,536**	**1,51,296**

.

VIII. CONCLUSION

This wok projected a hardware explanation for data embedding in color image using LSB and HAAR DWT image steganography schemeswith seven segment pattern which is used as a key for both embedding and extraction. Most of the existing random steganography techniques do not use the full capacity of the carrier image, while the proposed method uses the effective payload capacity of the carrier image and negligible distortion in the stego image. The same work is implemented on FPGA VIRTEX 6.From the experimental results it is observed thathardware speeds up steganography system than the software. Also thistechnique introduces the flexibility of changing the segment lengths, creating more difficulty in breaking the secret key. Moreover, it has been noticed that as the segment size increases, the PSNR value improves but the processing time increases. This system can be used for real time applications where processing time is not a major constraint.

REFERENCES

1) Mohammed Abbas Fadhil Al-Husainy "Full Capacity Image Steganography Using Seven-Segment Display Pattern as Secret Key" Journal of Computer Science, August 2018.
2) Nikhil Simha H.N "frequency domain Image Steganography using DWT and Modified LSB technique", IEEE International Conference on Advances in Computer Applications,ICACA,2016.
3) Abdullah AlWatyan, Wesam Mater, Omar Almutairi, Aisha Al-Noori, Sa'ed Abed "Security Approach for LSB Steganography Based" ,978-1-5090-5454, IEEE 2017.
4) Hamad A. A, Ali A, Majid A. A, Waleed A, "High Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data", IEEE Jordan Conf. on Applied Electrical Eng. and Comp. Tech., March 2015.
5) Chao Wang, Welming Zhang, Jiufen Liu and Nenghai Yu, "Fast Matrix Embedding By Matrix Extending" IEEE Transactions on Information Forensics and Security, Vol. 7, No 1, pp. 346-350, February 2012.
6) B. Vasantha Lakshmi and B. Videya Raju, "FPGA Implementation of Lifting DWT based LSB Steganography using Micro-Blaze Processor", International Journal of Computer Trends and Technology, Vol. 6, No. 1, pp. 6-14, December 2013.
7) Ran-Zan Wang and Yeh-Shun Chen, "High-payload Image Steganography using Two-way block matching," IEEE Signal Processing Letters, Vol. 13, Issue 3, pp. 161 – 164, March 2006.
8) B.J. Mohd, S. Abed, T. Al-Hayajneh, S. Alouneh "FPGA Hardware of the LSB steganography method," In Proc. of the IEEE International Conference on Computer, Information and Telecommunication Systems (CITS 2012), Amman, Jordan, pp. 5– 8, 2012
9) Shweta Modi and Meghana Kulkarni "FPGA Implementation of Transform Based Advanced Encryption Technique for Visual Cryptography" IJSTE - International Journal of Science Technology & Engineering Volume 2 | Issue 12 ,ISSN (online): 2349-784X, | June 2016
10) S. Mahmoud pour .s Mirzakuchaki, "Hardware Architecture for a Message Hiding Algorithm with Novel Randomizers," International Journal of Computer Applications, 0975 – 8887, Vol. 37-No.7, pp. 46-53, 2012
11) Maya C S, Sabarinath G, "An optimized FPGA implementation of LSB replacement steganography using DWT," International Journal of Advanced Research in Electrical , Electronics and Instrumentation Engineering, Vol. 2, special issue 1, pp. 586-593, 2013.
12) H. Patel, P. Dave "Steganography technique based on DCT coefficients," International Journal of Engineering Research and Applications, Vol. 2, Issue 1, pp.713-717, 2012.
13) Nikita Sharma and Meha Khera, " A novel approach to Image Steganography using Hash-LSB and DWT technique, International journal of advanced research in computer science and software engineering, Vol.5, Issue 6, June 2015.
14) Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh, Sahel Alounch, "FPGA Hardware of the LSB Steganography Methodl, IEEE Transaction on consumer Electronics, 978-1-4673-1550-0/12, 2014.

AUTHORS PROFILE

Savita D Torvi Research Scholar, Sri Siddhartha Academy of Higher Education, Maralur, Tumakuru, India.

K B ShivaKumar Professor and HOD, Department of Telecommunication Engg. Sri Siddhartha Academy of Higher Education.