 ISBN: 978-81-927230-0-9

An Efficient use of FPGA for Data Hiding:Survey

Latika R. Desai

Department of Electronics and Telecommunication Engineering, SPPU Pune.
Dr. D.Y. Patil Institute of Engineering and Technology, Pimpri, Pune, Maharashtra, India
latikadesai@gmail.com

Dr. Suresh N. Mali

Department of Electronics and Telecommunication Engineering, SPPU Pune.
Sinhgad Institute of Technology and Science, Narhe, Pune, Maharashtra, India
snmali@rediffmail.com

Abstract - ***We are using extensively digital data over internet or intranet, so there is need of secure and robust communication. While considering the security we have to consider different types of attacks. Attacks may be intentional or unintentional, passive or active. So while communicating we have to consent about data security. Data hiding plays vital role here to secure these communication or sharing the data, data on secure data pipe using hidden messages. This involves embedding data in to plain text, images, sound or video files and sending it over unsecure internet. Various Data hiding techniques used and tremendous research still going on and continues. Some of the examples like spatial domain, transform domain, etc. through our literature survey we observed that hardware technology gives us better result than software. In this paper we have mentioned need of data hiding in FPGA, literature survey of data hiding in FPGA, FPGA based data hiding technique based on previous researchers through different methodologies like spatial domain as well as transform domain and current state of art.***

Keywords— ***Data Hiding, FPGA, PSNR, Spatial, Transform.***

I. INTRODUCTION

In the today's information era, the need to protect the information is increasing continuously. In order to preserve important data in computer and communication systems from unauthorized access and again modification, reliable non-changeable means for data store and transmission must be assumed. Data hiding is an art of covered writing which means the information is hidden in a cover which may be audio or video or text or image. Many Data hiding techniques with image as cover have been proposed earlier which comes under two categories namely spatial domain and frequency domain. The last several decades it has seen fast growth of researcher's interest, in the field of data hiding. The main goal of reversible data hiding is to protect exact integrity of the original cover and data after extraction. This element is desirable when most sensitive data is present e.g. in Government, Military or medical imaging applications. Several reversible data hiding theories designed by researchers till now. A very high number of those theories or designs have been proposed for digital images. The people have constantly been trying to improve the capabilities of those reversible data hiding theories in terms of parameters such as embedding capacity, security, time complexity and robustness. The important data can be embedded either in spatial domain or frequency domain. Security, capacity, imperceptibility and robustness are essential features of a data hiding systems. The important data can be embedded either in spatial domain or frequency domain.

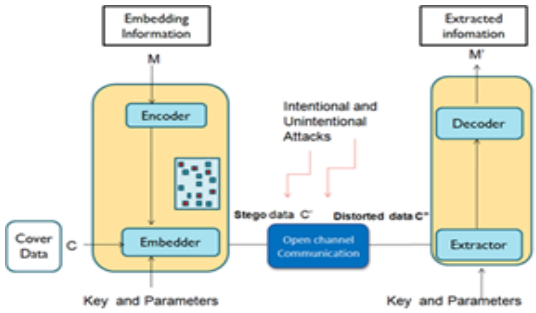

Fig. 1 General Data Hiding Module

Figure 1 shows the general data hiding module which consist of embedder and extractor embedder encodes data as per add key parameters than transfer to destination through extractor it decodes as per key parameters in between that some attack may happen to avoid that our embedding techniques should take care of it. The data hiding different techniques as explained below.

The Internet has revolutionized the modern world and the numerous Internet based applications that get introduced these days add to the high levels of comfort and connectivity in every aspects of human life [1][2]. Therefore, in the present information age, the need to protect the information is increasing rapidly. In order to protect valuable data in computer and communication systems from unauthorized disclosure and modification, reliable non vulnerable means for data storage and transmission must be adopted [3].Although encryption has been one of the solutions for information security, but encrypted messages once intercepted, can easily provide clue to the adversary or

attacker that some message of importance is being communicated. Data hiding, on the other hand, takes opposite approach and attempts to hide all evidence that communication is taking place[1]. The digital data hiding is a method used to hide or embed unique information into a digital image that can be uniquely identified later for its content and the authenticity [2].

Security, capacity, imperceptibility and robustness are essential features of a data hiding systems. Further, hardware implementations offers advantages over software realization in terms of less area, low execution time, low power, real time performance, high reliability and also ease of integration with existing consumer electronics devices [4]. The software designer does not have direct control over the way Random Access Memory (RAM) and processor interact, posing a limit on speed of execution of algorithm. On the other hand hardware designer have full control on total amount of RAM and required timing operations. Also, in any digital data hiding communication problem, if a chip is fitted in the digital device, the stego data signal can be obtained from the output of the source of signal at the origin. Manufacturing System On one Chip (SOC) for specific application is always expensive and takes long time to design. In contrast, programmable and reconfigurable solutions with Field-Programmable Gate Array (FPGA) are easy to implement with a short time with the help of Computer Aided Design(CAD) tools[5].No fixed architecture is likely to solve a large cross-section of the problem space very efficiently. FPGAs come into place for optimum implementation of algorithms since the architecture can be defined based on the application. Both connectivity and processing capabilities can be tailored to suit the characteristics of the problems. The majority of the chip used by a Central Processing Unit (CPU) of Personal Computer (PC) is not operating on each cycle [6-9]. In comparison, all of the hardware on FPGAs is executed in each clock cycle. FPGAs are more power efficient than CPU.

II. LITERATURE REVIEW

As a part of initial survey and finalizing the domain, focus was on study of data hiding methods for various applications. Summary of few papers are as follows:

Ingemar J. Cox et.al. [1], presented secure (tamper resistant), non-blind methodology for copyright protection using spread spectrum method. It can be extended for video watermarking. Maurice Maes et.al. [2], described copy protection methods for DVD Video. They claimed that encryption alone is not sufficient and also discussed issues in standardization of copy protection using watermarking. Ruizhen Liu et.al. [3], proposed a novel method for copyright protection using Singular Value Decomposition (SVD). This method works well in both security and robustness compared to Cox [1] method.

Gwena.elDo.err et.al. [4], given overview of various video watermarking applications They also covered various challenges in Video Watermarking than Image watermarking; like, i) attacks - there are many video processing's, which are likely to alter the watermark signal. ii) False Detection - resilience to collusion is much more critical in the context of video. iii) Real time - is often a requirement for digital video watermarking.They also pointed our various video watermarking trends and their pros and cons. One trend can be extension of image watermarking algorithm for video, problem with this can be computationally expensive. Another trend is using temporal or time domain approach; again problem is, computationally expensive and less robust. One more trend is using compression standard based approach; this is computationally effective but useful for the same compression standard.They suggested to combine various techniques and approached together for new real time challenging application. They mentioned the need of more research in this field for more robust and efficient video watermarking techniques.

Jeffrey Lubin et.al. [5],presented forensic watermarking approach based on spatio-temporal domain. They claimed that their method meets all three requirements, security, robustness and payload. PikWah Chan et.al. [6], proposed the novel algorithm, hybrid digital video watermarking, based on scene change technology and error correction code. They verified system resistant against attacks based on video characteristics and image processing techniques. They suggested enhancing the system by combining with audio watermarks for error correction capabilities and the hybrid scheme for attack resisting. Yinian Mao et.al. [7], presented techniques using signal processing and encryption for protecting multimedia data in MPEG format.

Sourav Bhattacharya, et.al. [8],performed a survey on available video watermarking techniques, feasibility study on watermarking techniques meeting application specific criteria for H.264/AVC and then performed a comparative analysis based on robustness and computational complexity of different watermarking algorithms.They concluded that most of the reliable and robust watermarking techniques are applied in transformed domain, so some modifications in the existing algorithms are required to implement watermarking in H.264 system. Lama Rajab et.al. [9], proposed two blind, imperceptible and robust video watermarking algorithms using SVD for copyright protection.

Y. Nakashima,et.al.[10],described a system for estimating the recording position from which a camcorder recording is made. The system is based on spread-spectrum audio watermarking for the multichannel movie soundtrack. The results indicate that the proposed system is applicable for practical uses. AlperKoz et.al.[11]taken a challenge of designing robust watermarking algorithm for free view video based on Image Based Rendering IBR. Min-JeongLee,et.al.[12] proposed a novel algorithm to find out position of pirate in cinema hall using pirated video. They used spread spectrum method. They are claiming that this algorithm is applicable to real time scenario. Dong-Wook Kim et.al.[13] reported problems of digital watermarking into intra frames of H.265/AVC using two blind and one semi-blind methods.

YujieZhang,et.al.[14], explained the new platform for professional video copyright protection. They used DCT, DWT and Neural Networks. They tested the platform for various copyright issues related to video, designed for MPEG Standard. They also concluded that at present only watermarking is not a complete solution for copyright protection, it needs other technical cooperation.[16-19], describes various video watermarking algorithms based on extension of image watermarking techniques. [20-25], presented information hiding through different techniques like LSB, DCT, DWT, simulation and implementation using FPGA and microarchitecture and its comparison also information hiding without loss of file formatting, combination of cryptography and steganography. [26-30], proposed the encrypting data with digital signature to prevent from attackers proposing dynamic method. Hybrid Steganography which is an integration of both spatial and transfer domain. The cover image as well as the payload, different algorithm implementation in FPGA using VHDL.

Ammar Odeh et.al [31], gives different strategies to protect data. Steganography techniques conceal information inside different digital media like image, audio, and text files. The technique used in this work is real-time Steganography technique to hide data inside a text file using a hardware engine that can achieve data rate in Gbps. The algorithm is better in language independency, hiding capacity. Scope defined is to parallel processing design to optimize, the system encryption speed and power consumption.

Mr Ning Liu ,et.al [32], demonstrated the hash-based randomized embedding algorithm that increases the security of the hidden data against the JPEG attacks. The derived mathematical expression for the security of algorithm can be increased independent of capacity, robustness, and embedding induced distortion. Here the maximum security depends only on the length of the key sequence, which is limited only by the size of the host image.

Mr Carlose and Mr Daniel Mozos [33], demonstrated an algorithm called N-FINDR. This is most popular and widely used algorithm though its high computational complexity when applied to high-dimensional images. He introduced a field programmable gate array design of the algorithm, which has been implemented on a Virtex-4 XC4VFX60 FPGA and evaluated using the well-known “Cuprite” image (a standard benchmark in hyperspectral imaging applications). Here hardware architecture has been implemented using VHDL language for specifying the N-FINDR module where the Xilinx ISE environment as well as Embedded Development Kit environment is used to specify the complete system and through which it retains excellent pure spectral extraction accuracy.

Mr Carlose ,et.al. [34], described a parallel implementation of the image space reconstruction algorithm which estimates positive fractional abundances in spectral unmixing of remotely sensed hyperspectral data with the help of Virtex 4 XCVFX60 FPGA through which it gives better optimizes input/output communication and its scalability. Scope mentioned here is there is possibility to modify the algorithm to make number of iterations per pixel adaptive for all the pixels that compose the hyperspectral image and by using better hardware resources we can decrease processing time. Magdy Saeb ,et.al.[35], presented a hardware adapted encryption the “PYRAMIDS” block cipher algorithm, hardware implementation using FPGA. Here the micro-architecture consists of two main functional blocks one is address control module which is used to generate and synchronize the memory address for reading the plaintext and writing the ciphertext operations and second is the encryption module it performs encryption operation. Better security achieved through this Micro architectures.

Ammar Odeh ,et.al.[36], presented a fast and real-time hardware implementation for secure and safe communications over networks. He presented the hardware implementation of the multipoint algorithm which gives the hardware implementation for text Steganography. Scope for further work is defined here, to present a parallel processing and design to optimize the system. [37-41], proposed 2/3 LSB Steganography which gives good image quality and facilitate simple memory access. Need to design more complex random based LSB mechanism as well as design speed and power. Also provides analysis of different parameters like Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR), Processing time, Security and through that it shows the BER and PSNR is improved in the LSB method but security sake DCT is the best method. DCT is highly secure and even the integrated approach of combining LSB and DCT. To implement steganography in hardware while in comparison between DCT and Wavelet-based algorithm by taking PSNR as parameter, both of them are robust but Wavelet based shows lower results. Here image data converted to binary data and embeds it to the carrier image.

Following figure 2 summarizes the literature survey,

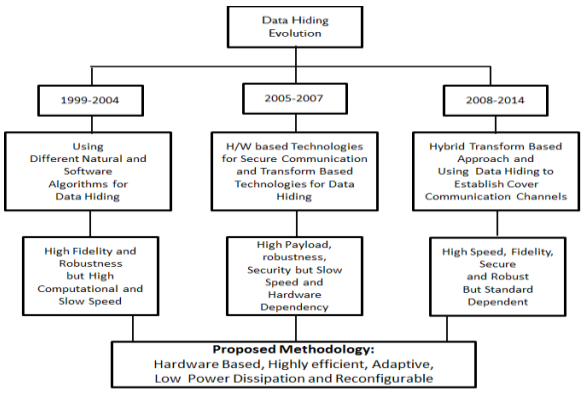

Fig. 2: Data Hiding Review

Demonstrated data hiding through DWT technique in FPGA[57], Genetic Algorithm in [58] while application of it through[59], hardware performance analysis details by [60], review details in[61] and different principles, applications given by[62]. Few more paper survey details are shown through table1 which are from year 2005 to 2014.

Sr. No.	Title	Year	Publication	Author	Method used	Advantages	Disadvantages
1	A survey on the application of FPGAs for network infrastructure security	2010	IEEE	Hao Chen ,Yu chen ,Douglas H. Summerville	Performance gap between speed of security and data processed handle by h/w implementation of security function and FGPA	Study of h/w based technique for security, signature detection, pattern matching	Require architectural and algorithm innovations
2	Distortion free image in image communication with implementation in FPGA	2012	Elesevier science	Santi Maity,Malay Kundu	Algorithm for Disortion free image in image communication and its VLSI realization using FPGA.	Low cost algorithm which speedup significantly by hardware realization.	NA
3	Releaving the Hidden Secret with LSB Steganography	2013	International Journal of Advanced research in Electrical, Electronics and Instrumentation Engineering.	Ankita Ganorkar	It used h/w design of LSB FPGA used for steganography.	Balanced imperceptibility, quality and capacity	Require to Improve design speed and power on h/w implementation.
4	Fast Real Hardware Engine For Multipoint Text Steganography	--	--	Ammar Odeh, Khaled Elleithy, And Miad Faezipour	Technique used to hide data inside a text file using h/w engine with 11.27 Gpbs data rate.	Fastest text stenography techniques in h/w	Optimize the system encryption speed and power consumption for multipoint algorithm[31]
5	An Improved FPGA Implementation Of The Modified hybrid hiding Encryption Algorithm (MHHEA) For Data Communication Security	2005	IEEE	Hala A. Farouk, Magdy Saeb	Comprehensive simulation and implementation result using FPGA and micro architecture. Combination of stenography and cryptography.	Micro architecture based on packet level Encryption.	Parallelism reconfiguration [21]
6	FPGA implementation of the “PYRAMIDS” block cipher.	2005	IEEE	Abdullah Alkalbany, Magdy Saeb	The PYRAMIDS block cipher is symmetric encryption algorithm of various length..H/w implementation sing FPGA	Adaptive or dynamic changing algo. Less space Secure processor structure.	Parallelism reconfiguration [35]
7	Stego System On Chip With LFSR Based Information Hiding Approach	2011	International Journal Of Computer Applications	R.Sundararaman, Dr. Har Narayan Upadhyay	Image stenographic system on FPGA. LFSR method used for hide the information in the image. **MSE** and **PSNR**.	High speed in secret data embedding at h/w level.	Enhancement of various bit wise function required.[4]
8	**Hardware Architecture for a Message Hiding Algorithm with Novel Randomizers**	2012	International Journal of Computer Applications	Saeed Mahmoudpour Sattar Mirzakuchaki	It is h/w realization of new **LSB** pseudo random number generator.	Protection against attack is improved. This allows image quality and message capacity adjusted accordingly user. secure	Parallel operation. [10]
9	FPGA Implementation Of X-Box Mapping For An Image Steganography Technique	2013	International Journal Of Advance Research In Electrical, Electronics And Instrumentation Engineering	Mr. Jagadeesh D.H., Mrs.Manjula, Dr.M.Z. Kuian	FPGA based on x-box mapping. x boxes having unique data.	Best quality and better security. Better for secret communication.	Pipelining [11]
10	Spatial domain image stenography based on security and randomization.	2014	International journal of advance computer science and application(IJACSA)	Namita Tiwari ,Madhu Sandilya,Dr. MeenuChawla	Increase the capacity of hidden data for security. result check on PSNR.MSE and capacity.	Highest capacity without distortion	Data hiding using randomization not possible.[44]
11	FPGA Hardware Architecture Of The Steganography Context Technique	2008	IEEE	Edgar Gómez-Hernández, Claudia Feregrino-Uribe, Rene Cumplido	Information hide in noisy region difficult to detect. LSB ,high speed.	High performance	Need of Repetitive operation.[20]
12	Survey And Analysis Of Hardware Cryptographic And Steganographic System On FPGA	2012	Journal Of Applied Science	S.Rajagopalan, R.Amirtharajan, H.Upadhyay,Jbalaguru Rayappan	Various algorithm study of C& S developed in software and hardware like FPGA .	High speed, low area, better efficiency over software	Improve security [45]
13	A Digital Image Steganography: Software & Hardware Approach	2013	International Journal Of Electronics and Communication Engineering	P. D. Gadekar & S. K. Waghmare	Steganographic technique using DWT for data hiding results gives differing by some little value.	Software &hardware approach	BF532 processor not that much efficient[46]

14	Adaptive Steganography based on textures	2007	International Conference on Electronics, Communications and Computers	Dulce R. Herrera-Moro, Raul Rodriguezguez-Colin, Claudia Feregrino-Uribe	Select texture is not homogeneous than difficult to detect information.	Reduce probability of detection	Easily message is lost. Improvement needed that is change the insertion method.[47]
15	FPGA Design for Pseudorandom number Generator based on Chaotic Iteration used in Information Hiding Application	2013	International Journal Applied Mathematics & Information Sciences.	Jacques M. Bahi	Pseudorandom generator	More Speed and secure	Internet security field area [48]
16	Matlab as a development environment for FPGA design	2005	*DAC 2005*, June 13–17, 2005, Anaheim, California, USA. Copyright 2005 ACM 1-59593-058	Tejas M. Bhatt	Design Flow from Matlab to FPGA	Development time reduced ,useful for RTL application	Design flow transition from floating point matlab to fixed point matlab . reduces simulation speed.

Table 1: Data Hiding methods with parameters comparison

According to literature review various the comparison of Least Significant Bit (LSB), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) techniques with respect to various features is as shown in Table 2.

Sr. No.	Parameters	Transform		Spatial
		DCT	DWT	LSB
2	Security	High	High	Low
3	Robustness	Medium	High	Low
5	Mean Square Error (MSE)	Low	High	Medium
1	Peak Signal to Noise Ratio	Medium	Low	Medium
4	Embedding capacity	Medium	Low	High

Table 2: Data Hiding methods with parameters comparison

As seen from literature review following are the main challenges observed in the existing available algorithm cannot handle all the parameters so we have to design system by keeping tradeoff between Capacity, security and Robustness.

III. CHALLENGES

As seen from literature survey and the motivation graph, following are the main challenges observed:

- Existing available algorithm cannot handle all the parameters.
- Always there is a tradeoff between Capacity, security and Robustness.
- Less attempts have been made with hardware reconfigurable parallel computing.
- Adaptive data embedding based on the attributes of cover data has also been missing.
- Effective utilization of FPGA blocks to accommodate complex logic required to hide the information for better security.

To handling massive data over internet it is necessary to maintain the confidentially and protect the information from various attacks. Here is an application of data hiding techniques to make this massive open channel data secured.

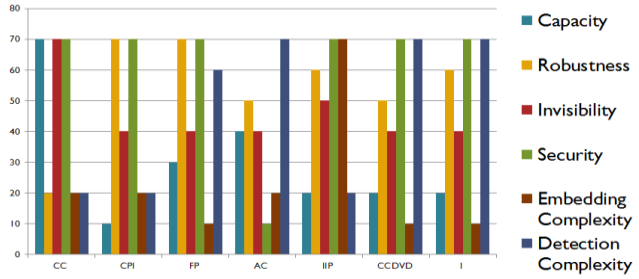

Figure 3: Motivation Graph-1

According to the above literature survey if we observed different applications as shown in figure 3 security is the major aspect used in all. So we are considered here security is the important parameter.

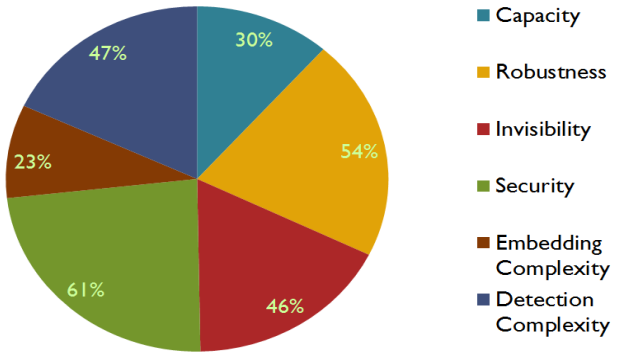

Figure 4: Motivation Graph-2

All these challenges motivates us to take this topic for our research wherein we can develop a system to enhance the security of digital content while optimizing all the data hiding parameters. As per the requirement few works is going on by using parallelism and block working still there is scope of improvement in security. Following table gives us work done from2014 to 2016 in different domains like spatial and transfer. Were they suggested the scope of further work like expanding the work to transform domain methods, such as DCT and DWTs, PSNR, etc.

IV. CURRENT STATE OF ART

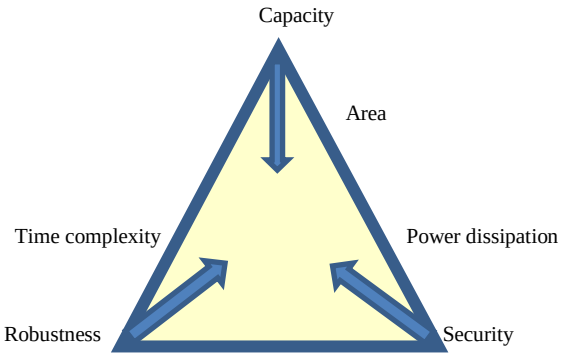

Figure 5: Triangle for Parameter Balance

As figure 5 shown from 2013 to till modification done by the different researchers in the data hiding techniques through architecture basis by keeping proper balance of capacity, robustness, security they trying to reduce area , power dissipation and time complexity. Still scope for enhamcement. Few of them stated here as, L. V. S Subbaraju el.at. [50] they provides an asymptotic upper-bound for the detection of hidden bits based on the LSB replacement mechanism where system is developed by using embedded development kit (EDK) tools on Xilinx Spartan3 field Programmable Gate Array (FPGA) device. Scope of future given through this work is Image processing system will be implemented on the Xilinx FPGA board using Xilinx EDK Tools. It will digitize and display on visual base window in a real time mode. Through this project, a hardware/software co-design method using FPGA will be explored for video and Image process applications.

Bassam Jamil Mohd, Sa'ed Abed, et. at.[51] presents innovative models to estimate energy-to-embed-secret-bit, peak signal-to-noise-ratio (PSNR) energy cost, power and resources in complex systems Future research should consider expanding the work to transform domain methods, such as DCT and DWTs. Also, it is important to analyze performance metrics from other platform flows (i.e., ASIC). Ammar Odeh Et. al [52] presented secure and safe communications over networks a with fast and real-time hardware implementation They provided the first hardware implementation which is presented in literature for text Steganography. Scope of future work is parallel processing design to optimize the system encryption speed and power consumption.

Balakrishnan Ramalingam et. al.[53] proposed a highly efficient ARIK LSB substitution scheme has been implemented in a cyclone II FPGA. They designed architecture which is operated at a frequency of 50 MHz, occupies 10513 logic elements and consumes 92 mW of power at the embedding stage. They achieved a reduced the computational overhead ,higher throughput and reduced power consumption in both stages encryption and substitution.

Bassam J. Mohd et. al [54] presented a novel algorithm in which without any secret bits loss embed and extract secret message. They discussed the FPGA-based hardware implementation of Wavelet-transform steganography the algorithm. as compare with other spatial domain designs this implementation is high cost implementation, with slower speed. This is due to transform domain involves complex computation operations, however, are more robust against statistical attacks. Scope of work mentined by them to enhance the PSNR of the stego-image.[55] used System generator and matlab approach.

Sr. No	Title	Year	Publication	Author	Methodology Used	PSNR	Scope Mentioned
1	Analysis and Modelling of FPGA Implementations of Spatial Steganography Methods	2014-2016	Journal of circuits system and computers	Bassam Jamil Mohd Hashemite University Thaier Hayajneh New York Institute of Technology	LSB	51.2	Expanding the work to transform domain methods, Such as DCT and dwts[51]
2	Wavelet-transform steganography: algorithm and Hardware implementation	2013-2016	Int. J. Electronic Security and Digital Forensics,	Bassam J. Mohd*, Thaier Hayajneh and Ahmad Nahar Quttoum	DWT	43.6	Improvement in PSNR[54]

3	Multiplexed stego path on reconfigurable hardware: A novel random approach	2015-2016	Sciencedirect , Elsevier Ltd.	Balakrishnan Ramalingam , Rengarajan Amirtharajan , John Bosco Balaguru Rayappan	MSB	54.08	NA[53]
4	Stego on FPGA an IWT approach	2014-2015	Hindawi Publishing Corporation Scientific World Journal	Balakrishnan Ramalingam, Rengarajan Amirtharajan, and John Bosco Balaguru Rayappan	IWT	63.18	Extended to develop a consecrated stego processor by means of FPGA Chip.[56]

Table 3: Current State parameters comparison

As demonstrated in the table 3 different current state of art with the security parameter. As shown in figure6 we can obsered that through IWT we are getting maximum PSNR. While in LSB and DWT. In [54] declare like expansion of work using transfer domain and still improvement of PSNR.

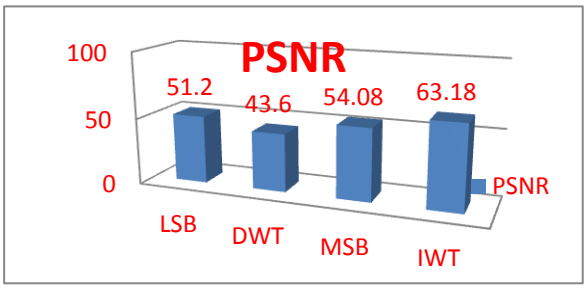

FIGURE 6 -Analysis and Comparison Through current State of Art

IV. CONCLUSION

The study of FPGA based data hiding technique demonstrated by previous researchers through various methodologies like spatial domain and transform domain. By analysing such a need of data hiding in FPGA and as per the literature survey, we observed that most of the work was done in LSB and therefore we can expand our work in transform domain methods, Such as DCT and DWT using FPGA. Because Still there is scope of improvement in PSNR. There is demand of architectural design for data hiding using FPGA. We have to design the system which should be a robust and secure one. There is a need to enhance the digital data by optimizing different parameters like robustness, vulnerability, etc. with adaptive digital data hiding mechanism in parallel reconfigurable modules of FPGA.

ACKNOWLEDGMENT

We are thankful to Dr. D. Y. Patil College of Engineering and Technology, Pimpri and Sinhgad Institute of Technology and Science for encouragement and support.

REFERENCES

1. Shabir A. Parah, Javaid A. Sheikh and G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique," IEEE International Conference on Emerging Trends in Science, Engineering and Technology, pp. 192-197, 2012.
2. G. Coatrieux, C. L. Guillou, J. M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," IEEE Transaction on Information Technology, Vol. 13, No. 2, pp. 158–165, 2009.
3. Dr.Ahlam Mahmood, Nada Kanai and Sana Mohmmad, "An FPGA Implementation of Secured Steganography Communication System," Tikrit Journal of Engineering Sciences, Vol.19, No.4, pp. 14-23, 2012.
4. R.Sundararaman and Har Narayan Upadhyay, "Stego System on Chip with LFSR based Information Hiding Approach," International Journal of Computer Application, Vol. 18, No.2, pp. 24-31, 2011.
5. E. Kougianos, S. P. Mohanty and R. N. Mahapatra, " Hardware Assisted Watermarking for Multimedia," Special issue on Circuits and Systems for Real Time Security and Copyright Protection of Multimedia, International Journal on Computer and Electrical (IJCEE), pp. 339-359, 2009.
6. Song Sun, "Analysis and Acceleration of Data Mining Algorithms on High Performance Reconfigurable Computing Platforms," Ph. D. Thesis, Iowa State University, pp. 11-11, 2011.
7. D. Bennett, "Is High Performance, Reconfigurable Computing the Next Supercomputing Paradigm," International Conference, Proceedings of the ACM/IEEE, pp. 15 –18, 2006.
8. Rupali Gawade, Priyanka Shetye, Vaibhavi Bhosale, and P. N. Sawantdesai, "Data Hiding using Steganography for Network Security," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 2, pp. 5740-5743, 2014.
9. R. J. Anderson and A. P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 474--481, 1998.
10. Saeed Mahmoudpour, Sattar Mirzakuchaki, "Hardware Architecture for a Message Hiding Algorithm with Novel Randomizers", International Journal of Computer Applications, Vol 37, No 7, Jan 2012.
11. Mr. Jagadeesha, Mrs. Manjula, "FPGA Implementation X-Box Mapping for an Image Steganography Technique", International Journal of Advanced Research in Electrical, Electronics, Instrumentation Engg. Vol.2 Issue 6, June 2013.
12. Magdy Saeb, Ramy Zewali, "A Micro-Architecture Implementation of YAEA Encryption Algorithm Utilizing VHDL & Field Programmable Gate Arrays", Proceedings of 3rd ICEENG Conference, May 2002.
13. Hao Chen, Yu Chen, "A Survey on the Application of FPGA's for Network Infrastructure Security", IEEE Communications Surveys & Tutorials 2010.
14. Himanshu Gupta, Prof. Ritesh Kumar, "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging Technology and Advanced Engineering Vol. 3, Issue 6 June 2013.
15. Shamin Ahmed Laskar, Kattamanchi Hemachandran, "Steganography based on Random Pixel Selection for Efficient Data Hiding",

International Journal of Computer Engineering & Technology (IJCET) Vol.4 Issue 2 , pp 31-44,March-April 2013.
16. Mamta Juneja, Parvinder Singh Sandhu, "A New Approach for Information Security using an Improved Steganographic Technique", J inf Process Syst Vol. 9 No 3, September 2013.
17. Stuti Goel, Arun Rana,"A Rewiew of Comparision Techiques of Image Steganography"' IOSR-JEEE, vol. 6, Issue 1, pp 41-48, May2013.
18. Elham Ghasemi, Jamshid Shanbehzadeh," "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", proceeding of the, Vol.1, IMCECS,Hong Kong, March 16-18, 2011.
19. K. B. Shivkumar. K.B. Raja, Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", IJCA(0975-8887), Vol.19, No.7, April 2011.
20. Edgar Gomez-Hernandez, Claudia Feregrino-Uribe, Rene Cumplido ,"FPGA Hardware Architecture of the Steganographic ConText Technique",18th ICECC,0-7695-3120-2/2008IEEE.
21. Hala A. Faroul, Magdi Saeb, "An Improved FPGA Implementation of the MHHEA for Data Communication Security", proceeding of the Design, 1530-1591/05, IEEE.
22. Po-Yueh Chen, Hung-Ju Lin, "A DWT based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006, Vol. 4 No-3, Page No 275-290, 2006.
23. H.B. Kekre, A. Athawale, "Performance Comparison of DCT and Walsh Transform for Steganography", International Conf & Workshop on Emerging Trends in Technology, 2010.
24. Maninder Singh Rana, Bhupender Singh Sangwan, "Art of Hiding: An Introduction to Steganography", International Journal Of Engineering And Computer Science Vol. 1, Issue 1, Page No. 11-12, Oct 2012.
25. Dr. S Sivasubramanian, Dr, Janardhana Raju, "Advanced Embedding of Information by Secure Key Exchange via Trusted Third Party using Steganography", International Journal of Latest Research in Science and Technology Vol., 2 Issue 1 Page No. 536-540,2013.
26. Dr. Suryakant Thorat, Mr. Madhav Bokare, "A Dynamic Method To Secure Confidential Data using Signcryption with Steganography", International Journal of Engineering Science and Advanced Technology [IJESAT] Vol.2, Issue 2, Page No.183-191,2012.
27. Hao Chen, Yu Chen, "A Survey on the Application of FPGA's for Network Infrastructure Security", IEEE Communications Surveys & Tutorials,2010.
28. K B Shiva Kumar, K B Raja, "Hybrid Domain in LSB Steganography", International Journal of Computer Applications Vol. 19, No 7, April 2011.
29. Deepak Singla, Rupali Syal, "Data Security Using LSB & DCT Steganography in Images", International Journal of Computational Engineering Research ISSN 2250-3005, 2012.
30. Selva Kumar, Thamarai P, "Network Data Security using FPGA", International Journal of Scientific Engg & Technology, Vol 4, Issue 5, May 2013.
31. Ammar Odeh , Khaled Elleithy , Miad Faezipour," A Reliable and Fast Real-Time Hardware Engine for Text Steganography"from www.researchgate.net/publication/262013703.
32. Ning Liu, Palak Amin, and K. P. Subbalakshmi, Senior Member, "IEEE ,Security and Robustness Enhancement for Image Data Hiding", IEEE Transactions On Multimedia, Vol. 9, No. 3, April 2007.
33. Carlos Gonz´alez, Daniel Mozos, Madrid Javier, FPGA Design of the N-FINDR Algorithm for Spaceborne Hyperspectral Missions,IEEE Journal Of Selected Topics In Applied Earth Observations And Remote Sensing, VOL. 5, NO. 1, February 2012.
34. Carlos González, Javier Resano, Member, IEEE, Antonio Plaza, Senior Member, IEEE, and Daniel Mozos, Member, IEEE, "FPGA Implementation of Abundance Estimation for Spectral Unmixing of Hyperspectral Data Using the Image Space Reconstruction Algorithm", Vol 5, Issue 1,February2012,IEEE.
35. Abdullah Kalbany, Hussein Ahma Hassan, Magdy Saeb "FPGA Implementation of The Pyramids Block Cipher", Science, Cairo University, Egypt, IEEE 2005.
36. Ammar Odeh, Khaled Elleithy, and Miad Faezipour ,"Fast Real Hardware Engine for Multipoint Text Steganography" Dept. of Computer Science and Engineering University Of Bridgeport Bridgeport, CT 06604, USA
37. Bassam Jamil Mohd, Saed Abed and Thaier AI- Hayaajneh, " FPGA Hardware of the LSB Steganograhy Method", 2012 ," IEEE Transaction on consumer Electronics,vol. 978, no. 1, pp. 4673–1550, 2012.
38. K.B. Raja, C. R. Chowdary and L. M. Patnaik, "A Secure Image Steganography
using LSB,DCT and Compression Techniques on Raw images", 0-7803-9588- 3/05/2005, IEEE.
39. Gurmeet Kaur and Aarti Kochhar**, "** A Steganography Implementation based on LSB & DCT", International Journal for Science and Emerging, ISSN No. 2250 3641,Vol.4, No.1, Page- 35-41,2012.
40. Shyam Sumukh S R, Raghav Gupta, Jagadish Nayak, "A Comparative Analysis in Hardware Partitioning of a Steganographic based LSB-substitution Algorithm", WCECS 2014,Vol I, 22-24 October, 2014, San Francisco, USA.
41. S. Saejung, A. Boondee, J. Preechasuk, " On the Comparison of Digital Image Steganography Algorithm Based on DCT and Wavelet", ICSEC, 2013,IEEE.
42. Santi Maity,Malay Kundu ,"Distortion free image in image communication with a implementation in FPGA ",International Journal of Electronics and Communications, Accepted 30 October 2012, Science Direct Elesevier.
43. Ankita Ganorkar1, Sujata Agrawal,,"Releaving the Hidden Secret with LSB Steganography", International journal of innovative research in electrical, electronics, instrumentation and control engineering,Vol. 1, Issue 3, June 2013.
44. Namita Tiwari ,Madhu Sandilya,Dr. MeenuChawla,"Spatial domain image stenography based on security and randomization", International journal of advance computer science and application(IJACSA), Vol 5, No 1,2014.
45. S.Rajagopalan, R.Amirtharajan H.Upadhyay,Jbalaguru Rayappan," Survey And Analysis Of Hardware Cryptographic And Steganographic System On FPGA", 2012
46. P. D. Gadekar & S. K. Waghmare," A Digital Image Steganography: Software & Hardware Approach", 2013.
47. Dulce R. Herrera-Moro, Raul Rodriguezguez-Colin, Claudia Feregrino-Uribe," Adaptive Steganography based on textures", International Conference on Electronics, Communications and Computers ,2007.
48. Jacques M. Bahi," FPGA Design for Pseudorandom number Generator based on Chaotic Iteration used in Information Hiding Application", International Journal Applied Mathematics & Information Sciences 2013.
49. Tejas M. Bhatt," Matlab as a development environment for FPGA design", DAC 2005, June 13–17, Copyright 2005 ACM 1-59593-058
50. L. V. S Subbaraju et al," A Hardware FPGA Implementation of Adaptive Stegano Analysis Using LSB Technique", Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.2010-2014 www
51. Bassam Mohd, Thaier Hayajneh, Sa'ed Abed and Awni Itradat ,"Analysis and modeling of fpga implementations of spatial steganography methods",researchgate.net/publication/259641931 February 2016
52. Ammar Odeh, Khaled Elleithy, and Miad Faezipour ,"A Reliable and Fast Real Time Hardware Engine for TextSteganography" , http://www.researchgate.net/publication/262013703 May2015.
53. Balakrishnan Ramalingam , Rengarajan Amirtharajan , John Bosco Balaguru Rayappan "Multiplexed stego path on reconfigurable hardware: A novel random approach", School of Electrical & Electronics Engineering, SASTRA University, Thanjavur 613401, India journal homepage: www.elsevier.com/locate/compeleceng Revised 12 February 2016.
54. Bassam J. Mohd*, Thaier Hayajneh and Ahmad Nahar Quttoums,"Wavelet-transform steganography: algorithm and hardware

implementation", International Journal of Electronic Security and Digital Forensics, Vol. 5, Nos. 3–4, pp.241–256., 2013.
55. K.N.Pansare, Dr. A.K.Kureshi," A Review-FPGA Implementation of Different Steganographic Technique", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 4, April 2014.
56. Balakrishnan Ramalingam, Rengarajan Amirtharajan, and John Bosco Balaguru Rayappan,"Stego on FPGA: An IWT Approach", Hindawi Publishing Corporation Scientific World Journal,Volume 2014.
57. Hemalatha Sa,1, U. Dinesh Acharyaa,"Wavelet transform based steganography technique to hide audio signals in image. Procedia Computer Science 47 (2015) 272 – 281.© 2015 The Authors. Published by Elsevier B.V.
58. Rinita Roy, Sumit Laha, "Optimization Stego Image rataining secret information using Genetic Algorithm with 8-connected PSNR, Published by Elsevier B. V. 2015.
59. Hao Chen, Yu Chen, "A Survey on the Application of FPGA's for Network Infrastructure Security", IEEE Communications Surveys & Tutorials 2010.
60. Sundararaman Rajagopalan, Siva Janakiraman, Har Narayan Upadhyay and K. Thenmozhi, " Hide and seek in silicon – Performance analysis of Quad block Equisum Hardware Steganographic systems", International Conference on Communication Technology and System Design 2011, vol. 30-2012, pp 806–813.
61. Satwinder Singh and Varinder Kaur Attri , "State-of-the-art Review on Steganographic Techniques" , International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.7 (2015), pp.161-170 http://dx.doi.org/10.14257/ijsip.2015.8.7.15.
62. J.Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2009.

Latika R. Desai , Research Scholor

Padmashree D.Y.Patil Institute of Engineering and Technology, Pimpri India..Total 17 years of Teaching Experience in Computer Engineering and Information Technology Department. Published 13 papers in various national and international journals conferences.

Dr. Suresh N. Mali is Principal, Singhgad Institute of Technology and Science, Narhe, Pune, India. He has written 3 technical books and published 57 papers in various national and international journals and various conferences. His areas of interest mainly include Steganography, Watermarking, Information Security, Data Hiding, Image Processing and Applications.