FPGA Implementation of New Data Transfer Data Matrix Methodology for IP Protection Scheme

Mrs. Nithyadevi
Assistant Professor
Department of Electronics & Communication Engineering
Dr. NGP Institute of Technology, Coimbatore, India

Ms. V. Gnana Merlin
UG Student
Department of Electronics & Communication Engineering
Dr. NGP Institute of Technology, Coimbatore, India

Mr. S. Kavin Kumar
UG Student
Department of Electronics & Communication Engineering
Dr. NGP Institute of Technology, Coimbatore, India

Ms. M. Mehala
UG Student
Department of Electronics & Communication Engineering
Dr. NGP Institute of Technology, Coimbatore, India

Mr. P. Mohan Kumar
UG Student
Department of Electronics & Communication Engineering
Dr. NGP Institute of Technology, Coimbatore, India

Abstract

Data matrix as a novel intellectual property (IP) protection technique can protect field programmable gate array (FGPA) IP's from the infringement. However, the data matrix technique will protect the sensitive information during the public verification. The third party vendors cannot crack the embedded watermark to resell the design. By the zero-knowledge watermarking verification schemes, we can address the sensitive information leakage issues but are vulnerable to embedding attacks, which makes them ineffective in preventing the infringement denying of verifiers. This paper proposes a new data transfer data matrix methodology based on the chaos based zero-knowledge interaction which resists embedding attacks. The proposed method with implementation result and analysis provided a high Secured data transfer with better robustness.

Keywords: Field Programmable Gate Array (FPGA), Intellectual Property (IP) Protection, zero knowledge, Data matrix

I. INTRODUCTION

Many types of Identities are existing in the human environment which can be utilized as the intellectual property (IP),they can be increased based on the reusable method, here the IP protection scheme protects the data from recording human visual perception result. The modular designed IP cores are easy to be copied or third parties can easily crack the embedded information and resell the design [2]. However, they created a compact implementation than software platform, mainly to limit the action of IP.

Field programmable Gate Array (FPGAs) are intended for their satisfactory performance, even they are compacted the zero turnaround time are at much lower volume when compare to ASICs[2]-[5].However, the FPGA faces the security issues for reprogramming, a file(bit-file)is loaded to Hardware for the essential programming.

II. EXISTING SYSTEM

To prevent the leakage of sensitive information from third party. The previous system provides a Zero knowledge verification which reduces the leakage issue in vulnerable embedded attacks and it limits verifiers.

A zero-knowledge protocol Verify ZKP to ensure trustworthy yet leakage-proof public verification based on the marks hidden in a FPGA design. Verify ZKP is fast, includes no additional design overhead, and needs no centralized signature database. It results on robustness.[3]- [8].IP protection solutions are usually limited to protect single FPGA configuration and require permanent secret key storage in the FPGA.

The general IP protection mechanisms to restrict the IP execution only on specific FPGA device. In order to protect IP from being cloned(or) copied, This mechanism enforce the pay-per-device licensing, which enable the system developers to purchase IP, that IP vendors embed argument finite state machines(FSM) into original IP such that the FSM can be activated by the PUF response from the FPGA [11].

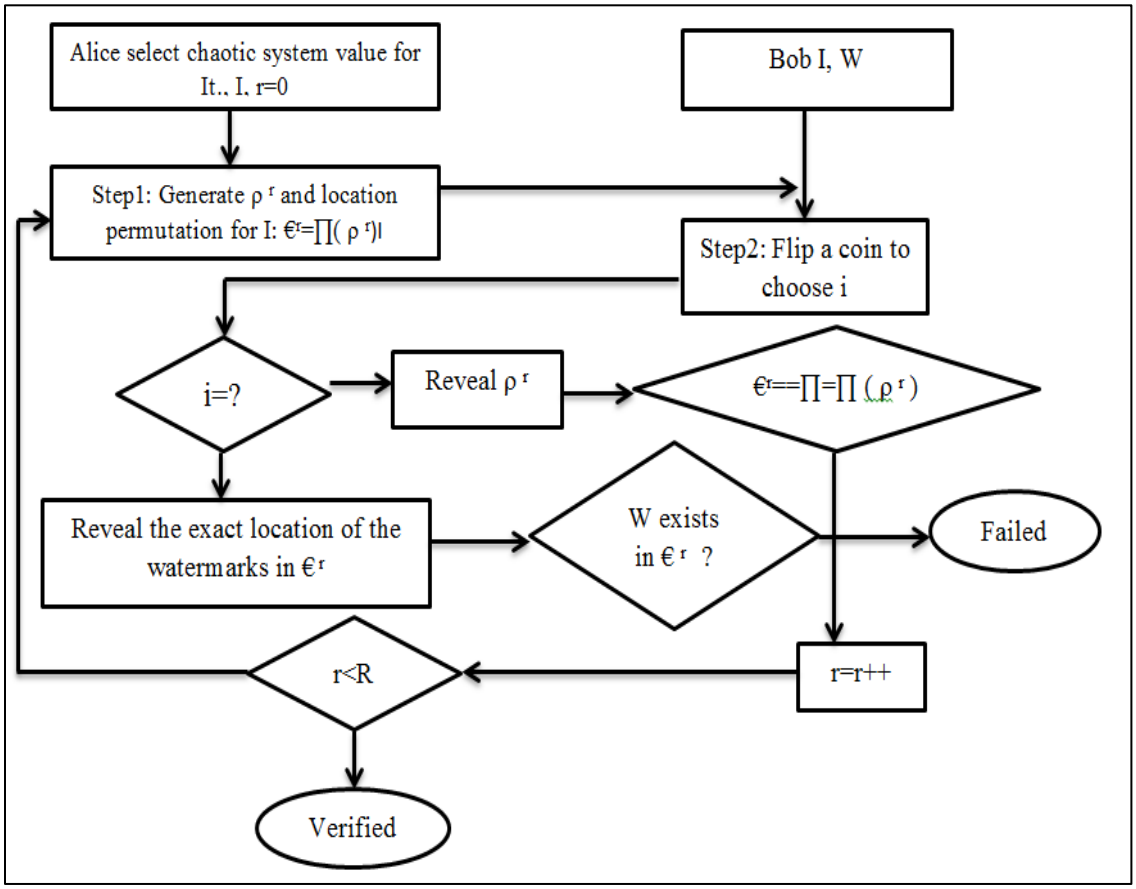

Fig. 1: Structure of the Existing Zero knowledge Verification Protocol between Alice and Verifier Bob.

III. PROPOSED SYSTEM

This paper focus on the new watermarking technology is taking the advantage of data matrix and the encryption keys. The data matrix not only recovers the original data, even when the data storage and barcode are damaged by the error checking and correction algorithm, it encrypts the original copyright information from the barcode. The encryption keys and the patterns are used to localize the watermark, and it creates an ability to work against the hacking attacks. [1] The Proposed method is to provide a secure data transfer of various kinds of intellectual property. It prevents the data from illegal copy and hacking. The data matrix sample is shown and the working module is shown below. The embedded functioning and the explanation of the module is explained with the reference.

Fig. 2: Data Embedded Image Representation – Data Matrix

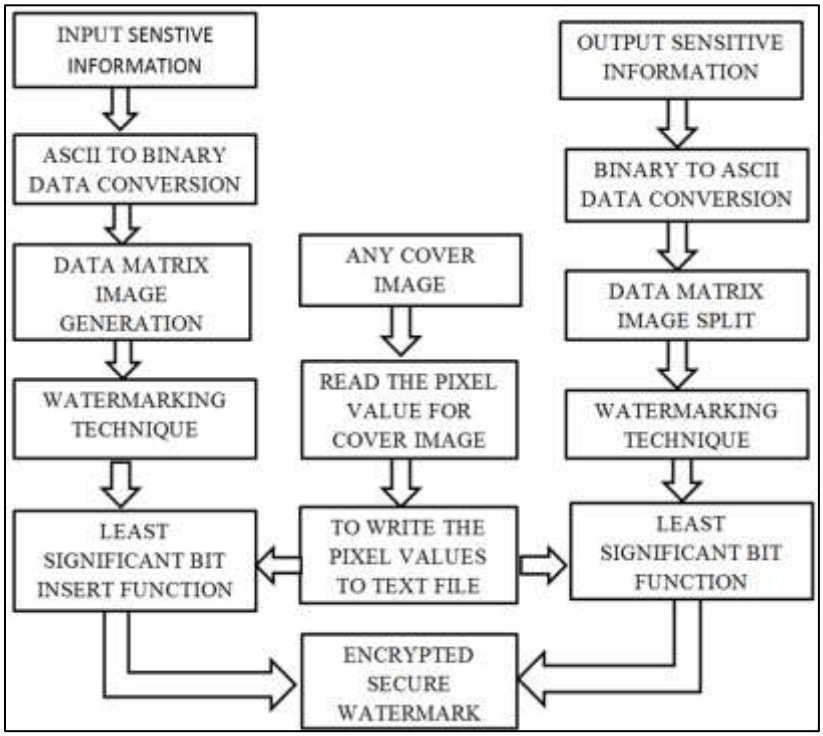

Fig.3. Block Diagram of Proposed Data Matrix System

The Proposed system splits into three different modules. The first module is referred the determined sensitive input data(trademarks, copyrights and Patterns)are modified and generated as encrypted keys and the telegraph codes (ASCII codes) are converted to the binary data's(01-10). The alphanumerical characters which are coded are generated as the data matrix image by(XOR Operation) .The information's are been embedded in an noise tolerant signal as audio and video to identify the ownership of the signal as watermarking[1].Any of the cover image is been taken, where the data to be embedded. By using the MATLAB the image pixel values are been noted and the image is generated as the grey level image [2].

The pixel values are written in the text file for the usage of LSB usage function. The binary data for the information is added with an LSB insertion function as, normal data (10000.101001.101101), LSB data (10001.101100.101100).


Fig. 4: Gray Level Image

The obtained sensitive output information is converted to binary data (alpha numerical) values, and the binary values are converted into telegraph codes (ASCII codes).With the timing pattern the data matrix splits the image to pixel representation. After the cover image splitting process the (WM) process is done to get the embedded data. Remove the LSB function to get the determined data format. The secured data format with the cover image is been encrypted for the data acquisition[11]-[14][1].The reverse process is done in the receiver side which first receives the image, then by the error checking and correction algorithm the embedded data is taken from the image, then by the encryption keys we can retrieve the original data[3].

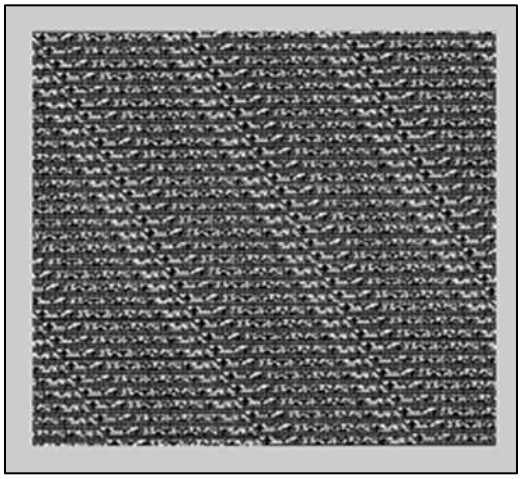

Fig. 5: Data Embedded Image

The Data Matrix technique is proposed to embedded both signature image and data on an original image. Performance is evaluated in term of peak signal to noise ratio (PSNR) and root mean square error (RMSE), image with fine details have higher PSNR and lesser RMSE and compared to images with a less information also a successful attempt has been made to hide a set of three signature images on the original images of large size. [10]

IV. IMPLEMENTATION & DESIGN

The low cost solution for bit stream security by adding authentication and encryption to the reconfiguration process using Authentication encryption. In addition to that using AES in 32-bit enhances the compact architecture. This can be use deficiently for secure configuration of FPGAs.

The XOR Gate is a digital logical gate that gives a true (1 or HIGH) Output when the number of true input is odd. XOR represent the inequality function. If both of its input are true, or if both of an XOR gate input are false then the output of the XOR gate is false. It explains the detailed barcode formation, the functional blocks are determined here; it's a 2x2 matrix in an entire data matrix block. The operation is explained with the 0's and 1's.It's a truth table expression from 000 to 111. The XOR operation retains the functional block the expression as follows,

SYMBOL	*TRUTH TABLE*
 2-input Ex-OR Gate *Boolean Expression* *Q= A+B*	*B* | *A* | *Q* *0* | *0* | *0* *0* | *1* | *1* *1* | *0* | *1* *1* | *1* | *0* *A OR B but NOT BOTH gives Q*

Fig. 6: XOR Gate of Data Matrix Implementation

Example: 010→0 the XOR operation provides a 0100; the three 0's determines the black box and the 1 determine the white box in functional blocks.

PARAMETER	*EXISTING SYSTEM*	*PROPOSED SYSTEM*
	CHAOS BASED KEY RANDOM METHOD	*DATA MATRIX WITH LSB TECHNIQUE*
SLICES COUNT	*3044*	*950*
LUT'S COUNT	*5584*	*1663*
DELAY TIME	*37.87ns*	*6.303ns*

Fig. 7: Output comparison Table

With the expressions and the algorithm proposed in the new system provides a better robustness than the existing system, with the provided results and comparison table is showed with a better results than the existing.

V. CONCLUSION

The data transfer data matrix methodology is proposed in this system to secure the Intellectual property. The sensitive method .The matrix method with the zero-knowledge verification helps in securing the data and IP protocols from the third party and advance hackers.

REFERENCES

[1] CHAUDHURY, CORDEL modeling anti-counterfeiting in 'response to protecting IPRIGHT'IEE VOL. 5, N.1, PP 59-72, 2015.
[2] H. Chang and L. Zhang, "A blind dynamic finger printing technique for sequential circuit intellectual property protection," IEEE Trans. Compute.-Aided Des.Integer. Circuits Syst., vol. 33, no. 1, pp. 76–89, Jan. 2014.
[3] A. Cui, G. Qu, and Y. Zhang, "Ultra-low overhead dynamic watermarking on scan design for hard IP protection," IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2298–2313, Nov. 2015.
[4] Daniel Zanier teach "Evaluation of watermarking methods for FPGA based IP cores in IEEE trans for computer aided, co design report 01 -2014
[5] C.GORMAN, "Counterfeit chips on the rise. IEEE spectrum vol. 49, no 6 pp, 16-17 June 2015.
[6] GUPTA R, Jain S, Mishara A, "Watermarking system for encrypted images at cloud to check reliability of images",(NGCT),Sept 2015.
[7] IAL-Aali, A.Teece, "towards the management of IP retrospective," IEEE Trans. Very Large Scale Integer. (VLSI) Syst., Jan.
[8] J. Kufel, P. R. Wilson, S. Hill, "Sequence-aware watermark design for soft IP embedded processors," IEEE Trans. Very Large Scale Integer. (VLSI) Syst., vol. 24, no. 1, pp. 276–289, Jan. 2016.
[9] A.B.KAHANG 'constraint based watermarking technique for IP design protection, IEEE TRANS NO 1O, pp1236-1252 ,0ct 2012
[10] Y.L.Lee "Signal rich art image-a new tool for automatic identification and data capture application", proc. IEEE Intl. conf. Acoustics speech and sig, proc 1997-1989,2005.
[11] Q. Liu, W. Ji, Q. Chen, and T. Mak, "IP protection of mesh NoC's using square spiral routing," IEEE Trans. Very Large Scale Integration (VLSI) Syst., vol. 24, no. 4, pp. 1560–1573, Apr. 2016.
[12] SAQUIB N,GUNAWAN T.S, Olanrewaju R.F ,Islam S Hassan M.K, "Qualitative analysis on watermarking algorithm for large resolution camera phone image", (ICCCE), Sep 2014.
[13] SPITZNER, "The honey net project of third party in IP SCHEME I" IEEE DES .VOL 30 NO 2, April 2013.
[14] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1137–1150, Jun. 2015.