Watermark Decoding Technique using Machine Learning for Intellectual Property Protection

Mr. R. Senthil Ganesh
Assistant professor-ECE, P.S.R Engineering College,
senthilganeshphd@gmail.com

Article History

Article Submission
21 May 2019
Revised Submission
15 July 2019
Article Accepted
19 August 2019
Article Published
30 September 2019

Abstract

The Watermarking is an Intellectual Property (IP) Protection method. It can ensure Field-Programmable Gate Array (FPGA) IPs from encroachment. The IP security of equipment and programming structures is the most significant prerequisite for some FPGA licensed innovation merchants. Advanced watermarking has become a creative innovation for IP assurance as of late. This paper proposes the Publicly Verifiable Watermarking plan for licensed innovation insurance in FPGA structure. The Zero-Knowledge Verification Protocol and Data Matrix strategy are utilized in this watermarking location method. The time stepping is likewise utilized with the zero-information check convention and it can versatility oppose the delicate data spillage and implanting assaults, and is along these lines hearty to the cheating from the prover, verifier, or outsider. The encryption keys are additionally utilized with the information lattice technique and it can restrict the watermark, and make the watermark vigorous against assaults. In this proposed zero-information technique zero rate asset, timing and watermarking overhead can be accomplished. The proposed zero-information watermarking plan causes zero overhead. In this proposed information lattice technique signal-rich-workmanship code picture, can be portrayed. The proposed information network watermarking plan encodes the copyright confirmation data. The zero-information confirmation convention and information grid technique proposed in this paper is executed by MATLAB R2014a in which C programming language is utilized in it and ModelSim 10.5b in which VHDL coding is utilized in it, are running on a PC. The combination instrument Xilinx ISE 14.5 is likewise used to confirm and actualize the watermarking plan.

Keywords: Publicly Verifiable Watermarking, Zero-Knowledge Verification Protocol, Data Matrix, Intellectual Property (IP) Protection

I. Introduction

The Watermarking is a huge field and a great deal of examination is going on around there. A blend of cryptographic methods, for example, encryption and watermarking together will give copyright insurance to pictures. By relying upon the expected prerequisites and the degree of security required, a proper watermarking calculation can be picked. The development of the Internet alongside the expanding accessibility of mixed media applications has generated various copyright issues and one of the territories that this development has powered is that of advanced watermarking. The Digital watermarking is the general method of installing a mass of data in the first document, with the end goal that a changed record is gotten. The mass of data along these lines included serves one of various uses, for example, distinguishing theft, detecting altering, or consoling respectability. The ways to deal with watermarking are different. It be extensively characterized dependent on their perceivability, power, or delicacy and their uses are additionally flexible as they can be applied to message, pictures, sound, or video [1].

ISSN: 2250-0839

The quick extension of the Internet in the previous years has quickly expanded the accessibility of advanced information, for example, sound, pictures and recordings to the general population and the issue of ensuring interactive media data turns out to be progressively significant. A great deal of copyright proprietors are worried about ensuring any unlawful duplication of the information or work. A portion of the genuine works should be done so as to keep up the accessibility of mixed media data. Be that as it may, meanwhile industry must think of approaches to secure licensed innovation of makers, merchants or basic proprietors of such information, this is a fascinating test and this is presumably why so much consideration has drawn toward the advancement of computerized pictures assurance plans. Of the numerous methodologies conceivable to ensure visual information, the computerized watermarking is presumably the one that has gotten most intrigue. The possibility of hearty watermarking pictures is to install data information inside the picture with a torpid structure for human visual framework. Yet, in the way, that shields from assaults, for example, regular picture handling activities and as the PCs are increasingly more incorporated through the system, circulation of advanced media is getting quicker, simpler. What's more, it requires less exertion to make precise however one of the significant obstructions is the absence of successful licensed innovation assurance of an advanced media, to debilitate unapproved duplicating and circulation [2].

II. Existing techniques

G. Qu [2002] built up the freely noticeable watermarking for IP confirmation in VLSI structure. This paper proposes a freely recognizable VLSI watermarking strategy that installs an autonomous open watermark for open check and the watermark is openly distinguished without losing its quality and security [1]. The possibility of this paper is to make a cryptographically solid pseudo-irregular watermark implant it into the first issue as a unique imperative and make it open. Lach et al [2001] built up a strategy for FPGA IP insurance. This paper proposes the method that use the novel attributes of FPGA to ensure business interest in IP through fingerprinting [2]. The covered up encoded mark is implanted into the physical format of a computerized circuit when it is put and steered onto the FPGA. This scrambled imprint exceptionally distinguishes both the circuit inception and unique circuit beneficiary.

D. Saha et al [2012] built up the open check of IP stamps in FPGA structures. This paper proposes the zero-information convention wherein it is an intuitive two-man game between the prover and the verifier. This convention fulfils zero-information property and acquaints factual measurements with measure its power [3]. The convention utilized in this is quick, brings about no extra structure overhead and needs no brought together mark database.

A. Cui et al [2015] built up the ultra-low overhead powerful watermarking on examine structure for hard IP insurance. This paper proposes ultra-low overhead watermarking plan to ensure hard IPs, the commanding type of business IPs. An improved sweep configuration utilizes two integral associations between two contiguous output cells and such sweep structure adaptability in the area of neighbourhood association styles gives a vehicle to install watermarking limitations [4]. It tends to be helpfully actualized by nearby reworking and additionally presenting sham sweep cells.

C.H. Chang et al [2014] built up a visually impaired powerful fingerprinting procedure for successive circuit IP assurance. This paper proposes the principal dynamic fingerprinting method on consecutive circuit IPs to empower both the proprietor and lawful purchasers of an IP implanted in a chip to be promptly distinguished in the field and the unique mark in this is an absent possession watermark autonomously supported by every client through a visually impaired mark convention [5]. Consequently the initiation can likewise be demonstrated through the identification of various clients' fingerprints without the need to independently implant an indistinguishable IP proprietor's mark in totally fingerprinted occasions. W.N. Falsehood et al [2006] built up the hearty and great time area sound watermarking. It depends on low recurrence sufficiency adjustment. This paper proposes a strategy for inserting computerized watermarks into sound signs in the time space [6]. This calculation abuses differential normal of total abundance relations inside each gathering of sound examples to speak to the slightest bit data and the guideline of low recurrence sufficiency adjustment is utilized to scale

amplitudes in a gathering way in chosen areas of tests so the time space waveform envelope can be nearly saved.

Y.L. Lee et al [2013] built up another instrument called signal rich craftsmanship picture for programmed recognizable proof and information catch applications utilizing cell phones. This calculation is made from a masterful objective picture to use as a transporter for a given message. This paper suggests that the made picture is outwardly like the objective picture, accomplishing the impact of sign rich craftsmanship and with its capacity like those of scanner tags or QR codes, such a kind of picture is delivered [7]. And afterward by dividing the making characters out of the message and infusing them into the objective picture by a novel picture square luminance adjustment conspire. Bassam Jamil Mohd et al [2012] built up the LSB steganography strategy. This paper proposes an equipment plan of Least Significant Bit steganography method in a twister II FPGA of the Altera family [8]. The equipment configuration uses the Nios implanted processor just as particular rationale to play out the steganography steps and the structure adjusts the tradeoffs, for example, impalpability, quality and limit.

Table 1: Comparative Analysis of some Existing Watermarking Techniques

MACHINE LEARNING ALGORITHM	ADVANTAGE	DISADVANTAGE
The combine data-integrity techniques are used in which it is compatible and resulting public-private watermark maintains the strength of watermark.	Easy detect ability and high credibility.	Low robustness is obtained.
The technique of cryptographically encoded marks to FPGA digital designs is used.	Capable of encoding long messages.	Performance and area impacts are minimal.
The fingerprinting based FPGA digital signature verification scheme is used.	Good robustness and overhead can be achieved.	Vulnerable to embedding attacks.
The ultra-low overhead watermarking scheme is used in-order to protect hard IPs.	Easy detect ability.	Low performance and vulnerable to embedding attacks.
The blind signature protocol is used for sequential circuit IP protection.	Applicable to both ASIC and FPGA IPs.	The robustness is low and low accuracy.
The time domain audio watermarking technique is used for embedding digital watermarks into audio signals.	High audio quality.	Low security is obtained.
The barcode image for automatic identification and data capture applications is used.	Good credibility.	The robustness is low and low security.
The least significant bit steganography technique for hardware design is used.	High quality.	Low robustness.

III. Proposed Methodology

With the predominance of reusable structure procedure in the IC configuration field, protected innovation (IP) encroachment turns out to be progressively genuine. A particular planned IP centers are anything but difficult to be duplicated or sold by outsiders without figuring out. In which it brings about colossal financial misfortunes to IP proprietors and lessens the piece of the overall industry of their items. Subsequently, how to forestall the IP encroachment successfully has become a tremendous test for field-programmable entryway exhibit (FPGA) sellers and IC originators. Be that as it may, the current watermarking procedures may part with delicate data during the open check, which empowers malevolent verifiers or outsiders to evacuate the inserted watermark and exchange the plan. Different watermarking check plans can address the touchy data spillage issue yet are helpless against implanting assaults, which makes them insufficient in forestalling the encroachment precluding from securing un-confided in purchasers (verifiers).

ISSN: 2250-0839

In this strategy, the new openly undeniable watermarking discovery conspire is proposed to address the issues that the FPGA watermarking procedure may release the touchy data and the current FPGA watermarking location plans are helpless against installing assaults. In this plan initial, a watermark is produced with the mark data and afterward the watermark is inserted dependent on the installing calculation. Next the asset, timing, watermarking overhead and the power of position stage of zero-information convention are examined. The confirmation plot proposed in this technique can, not just demonstrate that the watermark exists in IP without uncovering its substance and position, yet any verifier (counting un-confided in verifier) can check the authenticity of the watermark and oppose installing assaults against the cheating from the prover, verifier, or outsider adequately [9].

Since the computerized pictures are entirely helpless to controls and changes, an assortment of security issues are presented. For instance, the security place may wish to verify the information got from sensors spread over an office it should ensure. Another basic application is settling the proprietorship debates when copyrighted material is conveyed illicitly. Those issues and the requirements can be treated by installing a mystery imperceptible watermark (WM) in pictures. A WM is the extra distinguishing message, secured under the more noteworthy picture crude information, without perceptually transforming it and the expansion of a straightforward WM to the picture can be made conceivable to identify the adjustments exacted upon the picture, for example, trimming, scaling, covering, obscuring and some more. The WM can be included either a product stage or equipment stage, each having a few advantages and a few disadvantages, WM execution on an equipment stage experiences a constrained handling power contrasted with the product usage and it includes ongoing capacities and smaller usage. The upsides of the equipment WM usage are particularly upgraded in CMOS imagers, where it is conceivable to coordinate WM inserted solidly with the sensor cluster on a similar bite the dust [10].

In the current work, to forestall the spillage of delicate data and to upgrade the power of watermarking are finished by utilizing an enormous number of little watermarks rather than one huge watermark. In any case, this strategy will release a piece of the arrangement of watermarking positions after the open confirmation. At the point when encroachment happens over and over, more watermarking positions will be parted with, which encourages the assailant to expel more watermarks. The current freely perceptible VLSI watermarking procedures installs an autonomous open watermark for open check. Be that as it may, this strategy isn't reasonable for FPGA plans on the grounds that freely watermarking positions will be spilled after open confirmation, thus aggressors can alter, expel, or spread the open watermark in the bit-stream of FPGA structure, which would bring about an inappropriate check of IP. The reason for the open check is to diminish or wipe out the reliance of one gathering on the unwavering quality of different gatherings, decrease the requirement of the verifier in the convention and to improve the security of the whole plan. At the point when a debate happens among the gatherings engaged with the convention, open check is helpful for the intervention of a contest.
The procedure of watermarking age and inserting are as per the following.
Stage 1: Watermarking age - First, the mark S is scrambled with an encryption calculation. Second, the encoded S is attributed into a single direction Hash work, (for example, SHA-2) to produce a theoretical Swith fixed length. At long last, the watermark W is acquired by scrambling S with hashed tumultuous succession (the underlying estimation of the disarray is utilized as the key K1).
Stage 2: Locating watermark positions - Using a pseudorandom number generator, (for example, tumult K2 as the way) to create a pseudorandom arrangement as the watermark inserting positions.
Stage 3: The watermark is gathered by the most extreme estimation of the watermark in a LUT and afterward inserted into unused LUT of utilized Slice.
Stage 4: The information and yield of watermarked ILUTs are associated with the "couldn't care less" contributions of the first circuit so as to camouflage the inserted watermark.

ISSN: 2250-0839

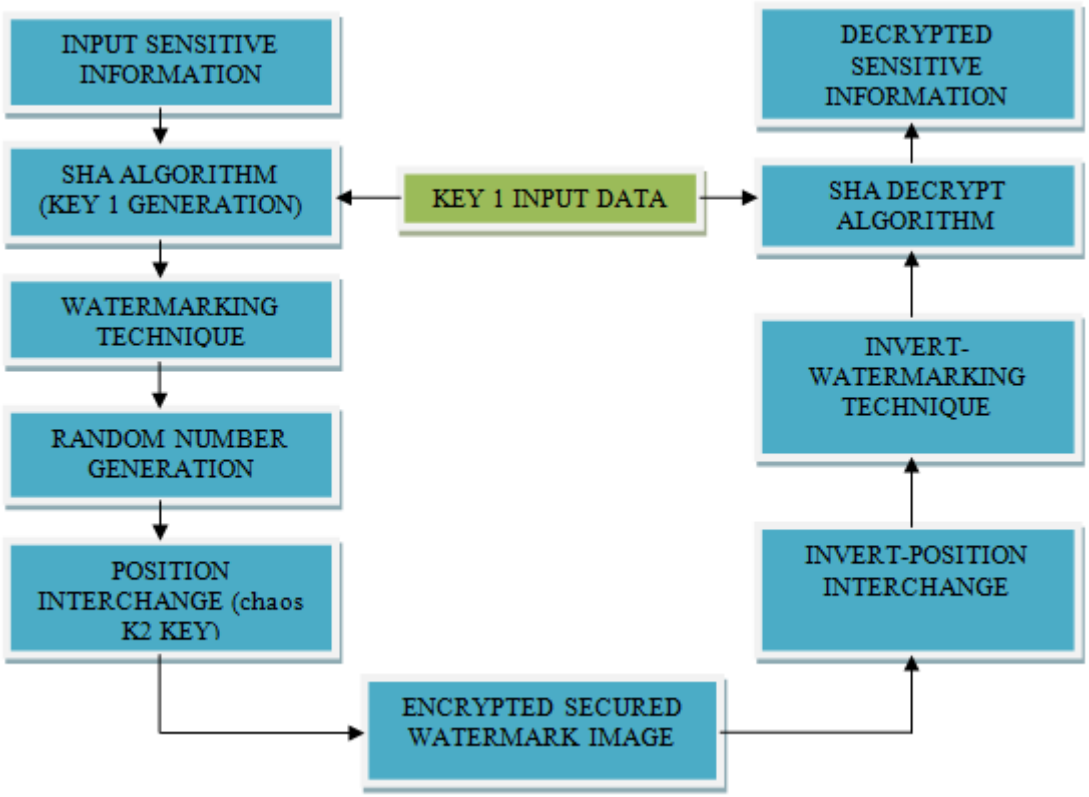

Fig 1: Watermarking technique using Machine learning algorithm

The Zero-information evidence or confirmation convention is a technique where a gathering A can demonstrate that given articulation X is surely consistent with party B without uncovering any extra data. Let say the Alice and Bob need to impart over shared system. The Alice starts the correspondence and sends mystery to Bob. Weave confirms the mystery so it tends to be sure that it is speaking with Alice. When it checks the mystery it sends adaptation. In the above situation, Bob must know Alice mystery so it can check Alice character however now Bob can mimic Alice. Zero-information convention permits Alice to demonstrate Bob that it knows the mystery without uncovering the mystery. In this convention the check procedure is performed for some executions and each time Alice needs to pass the confirmation. Zero-information convention is three pass recognizable proof convention. The main message is responsibility or witness sent from Alice to Bob, a subsequent message is challenge sent from Bob to Alice and a last message is reaction sent from Alice to Bob and if the announcement is genuine the legit verifier will be persuaded by the fair prover.

The zero-information convention has three properties. In the event that the announcement is valid, the genuine verifier will be persuaded by legitimate prover and it is called as Completeness. In the event that the announcement is bogus, Trudy can't persuade the verifier that it is valid, aside from with some little likelihood and it is called as Soundness. On the off chance that the announcement is genuine no swindling verifier gets the hang of something besides this reality and it is called as zero-information property. The Randomness is additionally a significant property of Zero information convention. Haphazardness in the responsibility and challenge message are utilized to shroud the mystery data. The professionals of the Zero-Knowledge Protocol incorporates, Secured (not requiring the disclosure of one's mystery and Simple (doesn't include complex encryption techniques). The Zero-information verification presents "The Knowledge Complexity of Interactive Proof-Systems". This strategy proposes the IP progressive system of intuitive confirmation frameworks and considered the idea of information unpredictability, an estimation of the measure of information about the verification moved from the prover to the verifier. It likewise gives the initial zero-information and an approach to dispose of the need of one way works. The single direction with multi-prover intelligent evidence frameworks

which have various free provers rather than just one, permitting the verifier to "interrogate" the provers in segregation to abstain from being deceived.

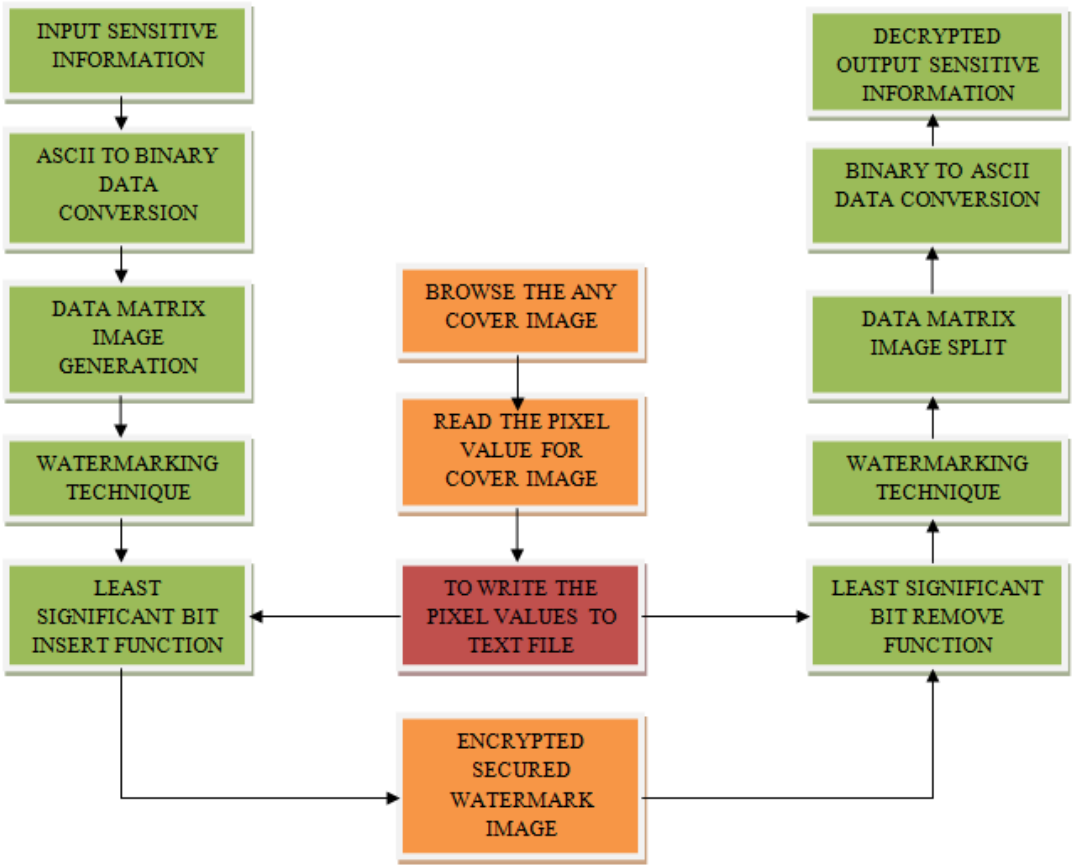

Fig 2: Watermarking technique using Data matrix method

Another watermarking method is exploiting Data Matrix just as encryption keys. The Data Matrix strategy not just recuperates the first information by a mistake checking and revision calculation, it even performs well when its high-thickness information stockpiling and scanner tag are harmed. It likewise encodes the copyright check data by randomization of the standardized identification, including proprietorship keys. In the information lattice strategy the encryption keys and the examples are utilized to limit the watermark and make the watermark hearty against assaults. By the correlation analyses of the copyright data removed from the watermark, it is conceivable to confirm that the proposed strategy has great quality and is hearty to different assaults, for example, JPEG pressure, separating and resizing. Data stowing away is significant piece of a wide range of techniques that are utilized to make information hard to take note.

This framework is to get information bits and make the information lattice design picture. This example picture implanted to any one chose picture utilizing rich workmanship code regulation technique. Another kind of sign rich-craftsmanship picture for uses of information move, called signal-rich-workmanship code picture, is proposed. The made code picture is outwardly like a pre-chosen target picture and with a given message installed, accomplishing the impact of the supposed sign rich craftsmanship. With its capacity like that of a QR code, such a sort of picture is created by encoding the message into a parallel piece stream, speaking to the bits by double code examples of 2×2 squares, and infusing the examples into the objective picture by a novel picture square luminance regulation plan. Each sign rich-workmanship code picture might be printed or shown, and afterward re-caught by a cell phone camera. Capable methods for checking the quantity of example squares and acknowledgment of code designs are additionally proposed for message extraction from the re-caught rendition of the sign rich-workmanship code picture. Great test results and a correlation of them with those of a current elective strategy show the achievability and prevalence of the proposed new information move technique.

IV. Simulation Results

The examination of inserting assaults incorporates the accompanying. An exploitative IP purchaser (verifier) utilizes an unapproved IP. A legit IP proprietor (prover) needs to demonstrate that the IP contains his watermark. In the real open check process, the verifier is frequently un-trusted in light of the fact that the verifier will endeavor to make a legitimate IP proprietor unfit to demonstrate his unlawful utilization of IP, i.e., despite the fact that the verifier utilizes the IP illicitly, the IP proprietor can't demonstrate it. Since FPGA IP is basically a piece stream document, a pernicious aggressor can install the watermark into the record. In this way, the current FPGA zero-information watermarking recognition frameworks are helpless against installing assaults. So as to forestall implanting assaults and disavowal of encroachment, we not just need to watermark the FPGA bit-stream, yet additionally guarantee the presence of the watermark before certain time.

Table 2: Resource Overhead Comparison

FPGA	Slices in original IP core	Existing method (previous watermarking techniques)		Proposed method (Zero-knowledge verification protocol)	
		Slices in watermarked IP core	Resource overhead	Slices in watermarked IP core	Resource overhead
XC2V250-6cs144	1231	1263	2.600%	1231	0%
XC2V1000-6bg575	2385	2417	1.342%	2385	0%
XC2V1000-6bg575	2538	2570	1.261%	2538	0%
XC2V1000-6bg575	3100	3132	0.946%	3100	0%

We can address the issue using the associating or spread trust time-venturing plan. The betray venturing plans can guarantee that paying little heed to how misleading the time-venturing organization (TSS) is, the events it ensures will reliably be the correct ones, and that it will be not ready to radiate base time-stamps. The scattered trust time-venturing plan even could be executed without the necessity for a concentrated TSS using any and all means. Right when a copyright banter occurs, the time that an attacker copies the IP unjustly and dispatches the embeddings ambush to embed the made watermark would slack in the ongoing. In the Analysis of Protocol Properties, the zero-data show should satisfy three properties - summit, adequacy and zero-data. The watermarking overhead is the mix of advantage and timing overhead and they are assessed by the used Slice and least clock period.

Table 2: Timing Overhead Comparison

FPGA	Minimum clock period in original IP core	Existing method (previous watermarking techniques)		Proposed method (Zero-knowledge verification protocol)	
		Minimum clock period in watermarked IP core	Timing overhead	Minimum clock period in watermarked IP core	Timing overhead
XC2V250-6cs144	17.123ns	15.210ns	-11.17%	17.123ns	0%
XC2V1000-6bg575	17.019ns	20.297ns	19.26%	17.019ns	0%
XC2V1000-6bg575	16.523ns	15.696ns	-5.01%	16.523ns	0%
XC2V1000-6bg575	16.310ns	16.838ns	4.63%	16.310ns	0%
XC6VCX75t-2ff484	13.578ns	14.106ns	3.24%	13.578ns	0%

The zero-knowledge verification protocol proposed is implemented by the software tools, MATLAB R2014a in which C programming language is used in it and ModelSim 10.5b in which VHDL coding is used in it, are running on a PC. The synthesis tool Xilinx ISE 14.5 is also used to verify and implement the watermarking scheme. The simulation results are obtained by the watermarking technique using zero-knowledge verification protocol (SHA algorithm) for intellectual property protection in FPGA design. This method involves the process of giving the input image and input text first and then it undergoes the encryption process by which the

encrypted secured watermark output image is obtained. Finally decryption process takes places and then the decrypted output is obtained.

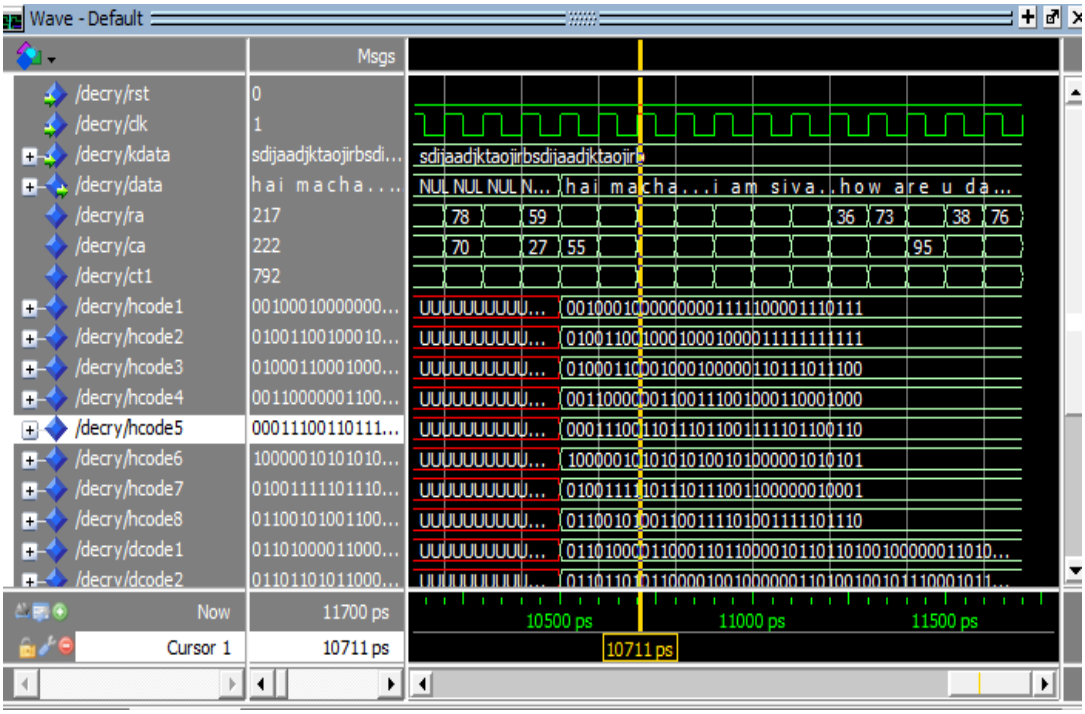

Fig 3: Simulation result of the proposed system

The data matrix method proposed is implemented by the software tools, MATLAB R2014a in which C programming language is used in it and ModelSim 10.5b in which VHDL coding is used in it, are running on a PC. The synthesis tool Xilinx ISE 14.5 is also used to verify and implement the watermarking scheme. The simulation results are obtained by the watermarking technique using data matrix method for intellectual property protection in FPGA design. This method involves the process of giving the input image first and then it undergoes the data matrix operations, LSB functions, encryption process by which the encrypted output image is obtained. Finally decryption process takes places and then the decrypted output is obtained.

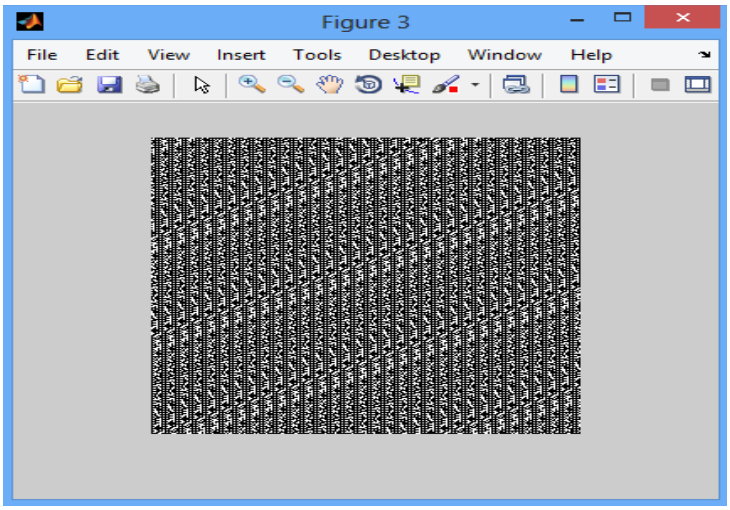

Fig 4: Simulation result showing watermark decoding using machine learning approach

V. Conclusion

The Machine learning watermark unravelling strategy and Data Matrix Publicly Verifiable Watermarking location conspire, proposed in this paper won't part with delicate data, for example, the substance and the situation of installed watermarks. Likewise, the connecting or dispersed trust time-stepping system utilized in zero-information check convention address the issue that the current FPGA watermarking location plans are helpless against implanting assaults. Since the intrinsic points of interest of the turbulent framework precisely meet the uncommon prerequisites of irregular position stage in the zero-information convention, the proposed conspire has high position change heartiness. In this proposed zero-information strategy zero rate asset, timing and watermarking overhead can be accomplished. The trial results likewise show that the proposed zero-information watermarking plan brings about zero overhead and the examination show that this strategy has preferable heartiness over the past watermarking procedures. The information grid watermarking plan proposed in this paper encodes the copyright confirmation data, including possession keys. The encryption keys and the examples utilized in the information framework strategy confine the watermark, and make the watermark vigorous against assaults. Another sort of sign rich-workmanship picture for uses of information move, called signal-rich-craftsmanship code picture utilized in the proposed information lattice strategy shows high predominance and attainability. The exploratory outcomes additionally show that the proposed information grid technique has great quality and the examination show that this strategy has great strength. The proposed zero-information and information framework technique additionally gives improved precision and execution level and it likewise decreases the unpredictability level. Subsequently this paper presents the work on the utilization of watermarking procedure for the IP security in FPGA plan.

References

[1] G. Qu, “Publicly detectable watermarking for intellectual property authentication in VLSI design”, IEEE Trans. Comput.-Aided Des.Integr. Circuits Syst., vol. 21, no. 11, pp. 1363–1368, Nov. 2002.

[2] D. Saha and S. Sur-Kolay, “Secure public verification of IP marks in FPGA design through a zero-knowledge protocol”, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 10, pp. 1749–1757, Oct. 2012.

[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] C.H. Chang, and L. Zhang, “A blind dynamic fingerprinting technique for sequential circuit intellectual property protection”, IEEE Trans. Comput.-Aided Des.Integr. Circuits Syst., vol. 33, no. 1, pp. 76–89, Jan. 2014.

[5] J. Zhang, Y. Lin, Q. Wu, and W. Che, “Watermarking FPGA bit-file for intellectual property protection”, Radio-engineering, vol. 21, no. 2, pp.764-771, Jun.2012.

[6] W. Liang, K. Wu, Y. Xie, and J. Duan, “TDCM: An IP watermarking algorithm based on two-dimensional chaotic mapping”, Comput. Sci. Inf. Syst., vol. 12, no. 2, pp. 823–841, 2015.

[7] Q. Liu, W. Ji, Q. Chen, and T. Mak, “IP protection of mesh NoCs using square spiral routing”, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 24, no. 4, pp. 1560–1573, Apr. 2016.

[8] B.Davis,“Signal rich art: enabling the vision of ubiquitous computing”, Proc. SPIE7880: Media Watermarking, Security, and Forensics III, N. D. Menon, J. Dittmann, A.M. Alattar, and E.J. Delp III, Eds., vol.788002, Feb.2011.

[9] F. Ernawan and M. N. Kabir, "A blind watermarking technique using redundant wavelet transform for copyright protection," 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA), Batu Feringghi, 2018, pp. 221-226, doi: 10.1109/CSPA.2018.8368716.

[10] P. T. Ngo and H. Quang Ta, "An Improved Blind Watermarking Technique Against JPEG Compression Attack," 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, 2018, pp. 189-192, doi: 10.1109/ATC.2018.8587565.

ISSN: 2250-0839