ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

A New Data Transfer Datamatrix Methodology for Digital Water Marking

Sathishkumar S, Gopalakrishnan G, M.E.,

Dept. of ECE, Mahendra Engineering College, Namakkal, India

AP, Dept. of ECE Mahendra Engineering College, Namakkal, India

ABSTRACT: Since digital images are very susceptible to manipulations and alterations, a variety of security problems are introduced. For example, a security centre may wish to authenticate the data received from sensors spread across a facility it is supposed to protect. Another common application is resolving ownership disputes when copyrighted material is distributed illegally. Those problems and needs can be treated by embedding a secret, invisible watermark (WM) in images. A WM is an additional, identifying message, covered under the more significant image raw data, without perceptually changing it. By adding a transparent WM to the image, it can be made possible to detect alterations inflicted upon the image, such as cropping, scaling, covering, blurring and many more. The WM can be added on either a software platform or a hardware platform, each having some benefits and some drawbacks. Although WM implementation on a hardware platform suffers from limited processing power, compared to the software implementation, it features real time capabilities and compact implementations. The advantages of hardware WM implementations are especially enhanced in CMOS imagers, where it is possible to integrate the WM embedded monolithically with the sensor array on the same die.

I. INTRODUCTION

The advance in semiconductor processing technology has led to rapid increase in integrated-circuit (IC) design complexity. Reuse-based design methodology has prevailed in IC design field. Intellectual property (IP) reuse can reduce product costs, shorten design cycles and decrease the design risk. Nowadays, reusable IP cores have become the basic units of system design. IP cores are widely exchanged and are being sold as an independent design. Most of reusable IP cores require a lot of time and effort to be implemented and verified by IP vendors, but these IP cores can be very easily copied or modified. Therefore, IP vendors are eager in keeping their products protective from unauthorized using and tampering. Additionally, users also expect that purchased IP core is correct and legitimate. How to protect reusable IP cores effectively has become a serious problem and therefore an increasing amount of attention has been paid.

Various kinds of IPP techniques, such as watermarking, fingerprinting, are proposed by researchers both from the industry and the academia. Among these techniques, watermarking is the most extensive mechanism implemented in the abstraction levels of IC design flow to protect IP cores from illegal reuse.

Current FPGA IP protection techniques can be roughly classed into two categories, active and passive. Active techniques devote to binding IPs on specific FPGA platforms to prevent infringement. Passive techniques mainly include bitstream encryption schemes and digital signature schemes. The bitstream encryption technique is to encrypt the configuration bitstream and then load it into an FPGA. For SRAM FPGAs, an FPGA design is stored in an external memory in the form of bitstream. Once the FPGA is started, the bitstream is loaded to configure the FPGA. In the configuration process, cloning the bitstream through the wiretap is possible. Digital signature-based scheme is to embed an encrypted signature (e.g., watermark or fingerprint) into an IP to represent the ownership. When the IP is suspected of infringement, the IP owner can apply for a trusted third party (TTP) to recover the signature from the IP to

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

prove the ownership. Digital signature is a novel technique applied to protect IP and has been widely studied for more than ten years.

In order to detect IP infringement, it will not be sufficient to focus on embedding the robust watermarks into IPs and detect the embedded watermarks effectively. Existing FPGA digital signature schemes verify marks by a designated verification team. However, it is difficult to ensure that all the members of the verification team are trusted in the real verification process. Therefore, the verification result announced by such a verification team may not be convincing to the IP buyer or IP owner. Correspondingly, for the public verification without the specified verification team involved, if the verifier can trace the marks embedded in IP, the verification result would be credible. However, in the public verification process, the prover will provide the sensitive information such as the content and embedded positions of marks to the verifier. Once the sensitive information is given away, malicious attackers can remove marks from the IP and then resell it. This is a serious threat to FPGA IP signature techniques. Furthermore, the FPGA IP is essentially a bitstream file. The embedded watermark or fingerprint in this file could be tampered with and covered more easily compared with ASIC. Public verification is a huge challenge in the field of FPGA IP watermarking, it is also one of the main obstacles to its application.

II. PUBLIC-PRIVATE WATERMARKING TECHNIQUE

Watermarking and fingerprinting are indirect protection schemes in that they provide a deterrent to infringers by providing the ability to demonstrate ownership of an IP to its originator. However, establishing the ownership is challenging as we have discussed earlier.

Watermark Creation: The proposed public–private watermark consists of two parts: public and private, which are selected separately. We inherit the private part of the watermark from the traditional digital watermark discussed in early works. A typical watermark is a cryptographically strong pseudo-random bit stream created by crypto systems using designer's digital signature as the secret key. For example, we can hash the plain text message to get a 128-bit or higher hash result. We then apply a stream cipher to make the same plain text message pseudo random using the above hash result as the key. The public watermark has a header and a body that are both derived from a short plain text message such as the four- or three-letter symbol for the design company. The ASCII code of this short text is used as the public watermark header. The public watermark body, which is a pseudo-random bit stream, is created exactly the same way as we build the private watermark.

Watermark Embedding: Watermark embedding is the process of translating the watermark, a pseudo-random bit stream, into design constraints. The public and private watermark can be embedded by either the same encoding scheme or different ones. The development of such schemes requires us to explore the characteristics of the given problem and we will discuss this in Section IV on several specific VLSI CAD problems. However, to ensure the detectability of public watermark, we must make the following public: 1) the one-way hash function being used in the construction of public watermark; 2) the (public) watermark encoding scheme being used to create the constraints; and3) the place where we embed these (public watermark related) constraints. We keep the secret key out of the reach of public to make the private watermark secure1.

Watermark Detection: The public watermark can be detected from the following public information: 1) the hash function; 2) the watermark scheme; and 3) the place that hosts the (public) watermark. First, we check for the existence of constraints in the hosts for public watermark and obtain the entire public watermark message. Next, we extract the message header (since its length is known), which is the designer's public signature in ASCII. Then, we can hash this message header for further verification of the authorship. A match of the message header with designer's publicly known signature gives the first level proof of authorship. A match of the message body with the new hash result will establish stronger proof. Finally, further evidence can be shown when the secret key (for the private watermark) is available or forensic tools can be used to detect the private watermark by the existing copy detection techniques.

Watermark Robustness: Unlike the private watermark, which is as secure as before, the public watermark is visible to the public and may be vulnerable against attacks. In most known watermarking techniques, attackers will have a great amount of advantage if they can detect the watermark. The public watermark exploits the concept of data integrity to prevent this. To be more specific, a forgery is successful if the adversary can replace the original public watermark by

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

his public information. The adversary can create his own public watermark using the published hash function. Then he can alter the constraints based on the public-known watermark encoding scheme and embed them in the specific places. Finally, he modifies the known solution, which satisfies the original public watermark, to meet his faked public watermark constraints. Now a successful forgery is built! However, this is unrealistic2 , if not impossible, due to two facts: 1) the faked hash will be different from the original in half of the bits statistically even if the message header is changed only by one bit, which is significant if we make the message body sufficiently long. 2) the design integrity implies that even one small local change may alter the behavior of the design, which means that any forgery will require some level of local modification.

III. RELATED WORK

Many current IP protection techniques are based on encrypted source files. For example, encrypted HDL modules disguise the form and structure from IP users. This allows the IP users the ability to incorporate soft modules and high performance simulation models into their design using a CAD tool provided with the decryption key, without exposing the IP to theft. However, this approach has been routinely and successfully attacked, often by directly attacking the CAD tool. Therefore, there is no foreseeable IP protection technique based on encrypted source files, despite stronger forms of encryption and more thorough systems engineering.

Signature hiding techniques for image, video, and audio signals have recently received a great deal of attention. Digital image steganography has been especially well explored. Although many mark security and verification issues have been raised, several image watermarking techniques do exist that have been shown to be robust against all known attacks. Digital audio protection has proven to be even more difficult, but many different techniques have nevertheless been proposed. Video stream protection techniques have also been developed. Techniques have arisen that provide general intellectual property protection through watermarking. Marks are embedded at the behavioral level down to the physical layout by imposing design constraints phases (physical synthesis of FPGA-based design vs. behavioral synthesis). Addressing the design at a lower level of abstraction provides the advantage of a larger design space and greater flexibility, making it possible to embed signatures that are significantly more difficult to detect and remove.

To prevent the leakage of sensitive information, Existing work to enhance the robustness of watermarking using a large number of small watermarks instead of one large watermark. However, this method will leak a part of the set of watermarking positions after public verification. When infringement occurs repeatedly, more and more watermarking positions will be given away, which facilitates the attacker to remove more watermarks. Existing a publicly detectable VLSI watermarking technique that embeds an independent public watermark for public verification. However, this method is not suitable for FPGA designs because public watermarking positions will be leaked after public verification, hence attackers can tamper, remove, or cover the public watermark in the bitstream of FPGA design, which would result in the wrong verification of IP.The purpose of public verification is to reduce or eliminate the dependence of one party on the reliability of the other parties, reduce the constraint of the verifier in protocol, and improve the security of the entire scheme. When a dispute occurs among the parties involved in the protocol, public verification is convenient for the arbitration of dispute.

IV. PROPOSED WORK

In this paper, a new publicly verifiable watermarking detection scheme based on chaotic sequences is proposed to address the issues that the FPGA watermarking technique may leak the sensitive information and the existing zero knowledge FPGA watermarking detection scheme is vulnerable to embedding attacks. This scheme comprises the following.

1) The watermark is hidden in the unused lookup table (LUT) of used Slice, and the watermarking content of LUT of ˆ I is encrypted to prevent the leakage of watermarking content.

2) Since chaotic sequences have high randomness and low cross correlation, we can generate a real number chaotic sequence in each round of verification. The chaotic sequence is binarized into ρ, which is used as an input to the position mapping algorithm $\pi(\rho)$ to control the location permutation of LUTs in FPGA bitstream, i.e., $\pi(\rho)$ is applied to

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

ˆ I to get the scrambled design ξ. Then ρ and the position of the watermark in ξ are used to interact between the prover and verifier. With the zero knowledge protocol, the prover makes the verifier believe the watermark existing in IP without leaking the position information.
3) Timestamp is introduced to resist embedding attack to prevent dishonest IP buyers from denying.

A new watermarking technique taking advantage of Data Matrix as well as encryption keys. The Data Matrix not only recovers the original data by an error checking and correction algorithm, even when its high-density data storage and barcode are damaged, but also encrypts the copyright verification information by randomization of the barcode, including ownership keys. Furthermore, the encryption keys and the patterns are used to localize the watermark, and make the watermark robust against attacks, respectively. Through the comparison experiments of the copyright information extracted from the watermark, we can verify that the proposed method has good quality and is robust to various attacks, such as JPEG compression, filtering and resizing.

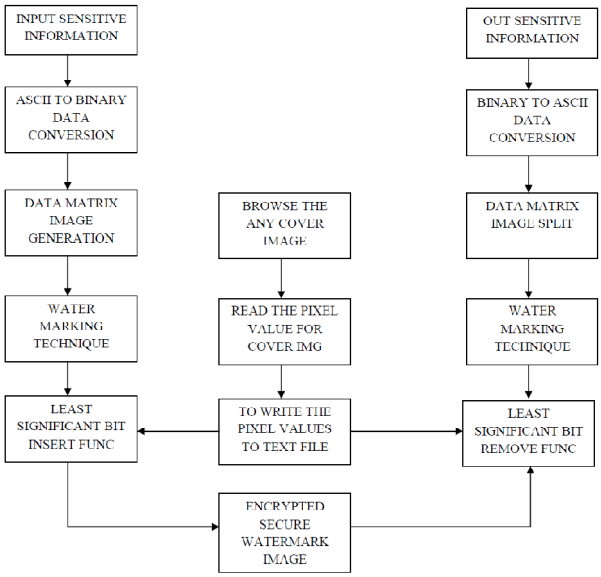

Fig 1: Block diagram

Proposed Algorithm:
1: Select cover image and secret image
2: Convert both RGB image into three elements- red, inexperienced and blue.
3: Perform 3-DWT at red image to split it into 4 coefficient units: h_LL, h_HL, h_LH and h_HH.
4: Perform 3-DWT once more on h_HL and h_LH coefficient units to get smaller coefficient sets and select 4 coefficient units: h_LL1, h_HL1, h_LH1 and h_HH1.
5: split 4 coefficient sets: h_LL1, h_HL1, h_LH1 and h_HH1 in 4 x 4 blocks.
6: Apply DCT to each block in selected coefficient units (h_LL1, h_HL1, h_LH1 and h_HH1). These coefficients sets are selected to look if each of imperceptibility and strength of algorithms similarly.
7: Perform 3-DWT on the secret red image to divide it into four coefficient sets: s_LL, s_HL, s_LH and s_HH.
8: Perform 3-DWT again on s_HL and s_LH coefficient units to get smaller coefficient units and select four coefficient sets: s_LL1, s_HL1, s_LH1 and s_HH1.
9: split 4 coefficient sets: s_LL1, s_HL1, s_LH1 and s_HH1 into 4 x 4 blocks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

10: Apply DCT to every block in the chosen coefficient sets (h_LL1, h_HL1, h_LH1, h_HH1 and _LL, s_HL, s_LH and s_HH). These coefficients sets are decided on to look if each of imperceptibility and energy of algorithms equally.
11: Apply opposite DCT (IDCT) on every block subsequent to its mid-band coefficients contain been altered to implant watermark bits as defined within former step.
12: Apply the inverse 3-DWT (3-IDWT) on the 3-DWT distorted image, including the customized coefficient sets, to make the watermarked cover image.

V. RESULT

Here we using ModelSim and Matlab to simulate the system. Matlab used to convert the image to text file and in modelSim we read the values and process it.

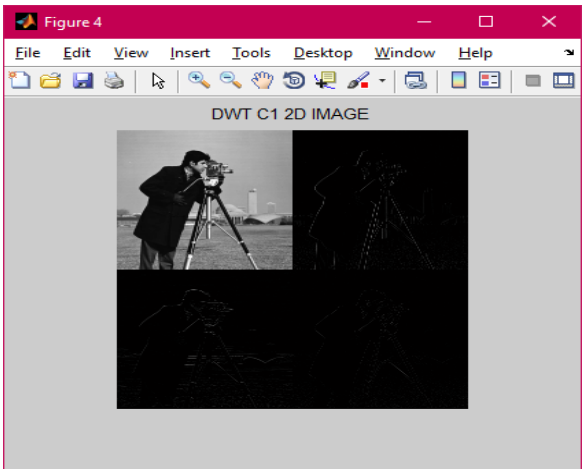

Fig 2: DWT of Input Image

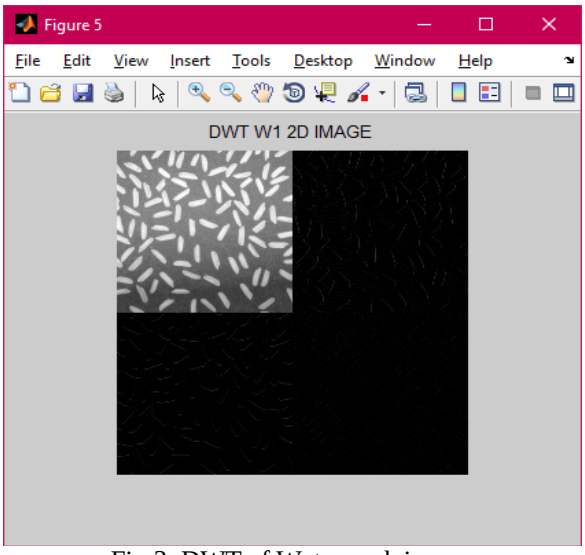

Fig 3: DWT of Watermark image

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

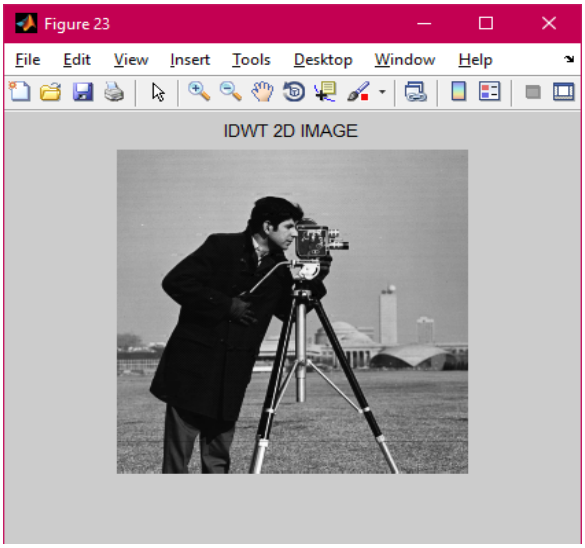

Fig 4: IDWT of Cover image

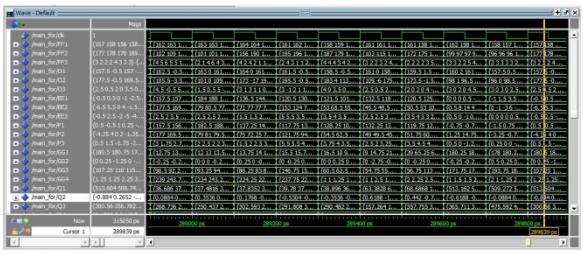

Fig 5: Simulation result

VI. CONCLUSION

The chaos-based publicly verifiable watermarking detection scheme proposed in this paper will not give away sensitive information such as the content and the position of embedded watermarks. In addition, the linking or distributed trust time stamping mechanism is used to address the issue that the existing FPGA watermarking detection schemes are vulnerable to embedding attacks. Since the inherent advantages of the chaotic system exactly meet the special requirements of random position permutation in the zero-knowledge protocol, our proposed scheme has high position permutation robustness. The experimental results also show that the proposed watermarking scheme incurs almost zero overhead. In our proposed zero-knowledge verification protocol, each round of protocol will generate a new chaotic sequence for random position permutation and the sequence will be discarded at Step 5. Step 1–Step 5 must be executed *R* rounds in order to reduce the probability that Alice succeeded in deceiving Bob. Assuming the number of public verification is *M*, the number of random permutations would be *M***R*. The empirical value for *R* is 128 because it is sufficiently secure (against brute force attacks). However, it is difficult to give an empirical value for *M*, because the value of *M* depends on the times of IP infringement. Besides, in order to ensure the security, the correlation between these random permutations should be extremely low. However, analogous to related works, it is difficult to give an empirical value for "extremely low." In the future work, it is significant to give the empirical values for them.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

REFERENCES

[1] M. A. Gora, A. Maiti, and P. Schaumont, "A flexible design flow for software IP binding in FPGA," *IEEE Trans. Ind. Informat.*, vol. 6, no. 4, pp. 719–728, Nov. 2010.
[2] 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.
[3] S. Trimberger, J. Moore, and W. Lu, "Authenticated encryption for FPGA bitstreams," in *Proc. ACM/SIGDA Int. Symp. Field Program. Gate Arrays*, 2011, pp. 83–86.
[4] 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.
[5] 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.
[6] 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.
[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] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "Robust FPGA intellectual property protection through multiple small watermarks," in *Proc. 36th Annu. ACM/IEEE Design Autom. Conf.*, Jun. 1999, pp. 831–836.
[9] 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.
[10] J. Zhang, Y. Lin, Q. Wu, and W. Che, "Watermarking FPGA bitfile for intellectual property protection," *Radioengineering*, vol. 21, no. 2, pp. 764–771, Jun. 2012.