The Watermarking Method Based On RNS For Uphold The Publisher's Law

Sajjad Bagheri Baba Ahmadi, Yaser Ahangari Nanehkaran

Abstract: - In recent years, as for daily spread of communications in the world, there has been an increasing interest in protecting data and information against copy and counterfeit. For this we have to use solutions for controlling copy and counterfeit .The Watermarking method is one of the more practical ways of uphold the publisher's law . Generally, The Watermarking Method means hide the data in a cover for exert ownership right that only admissible people can extract this data. This paper will focus on and propose the way of protect ownership right based on the multilevel-residue number system (RNS).The aim of this study is protect publishers' law , with reusable ability via create a digital signature that after it's created , can be embedded in un-use positions of look-up tables of RNS-based designs. This type of embedding does not increase the area of the system .The paper also render a technique for extract digital signature. So, the issue is possible to recognize publisher's law without any disturbance in the system operation.

Index Terms: - Digital Signature, Digital Watermarking, Euclid's theorem, N-Channel CRT, Residue Number System, Watermarking, HDL design.

1 INTRODUCTION

DAY by day as the offices without paper expand and as the size of internet grows, so most of document and data make and offer in form of digital data. Digital nature implies that create, modify, update, share, store and disseminating information are easier than before, So as much abuse of data is more. It require a technique to provide the ways to authenticate users to prove their ownership on digital content and prevents to tampe-ring and distribution of the data illegally by the unauthorized users. Currently many tools are easily available which can modify or duplicate the data either it's image, video, audio or text. So to achieve security requirement the useful technique is known as digital watermarking. Conventional methods that based on watermarking sup-porting hardware and media by inserting a watermark in data. In a way that it is difficult to change or remove the watermark. Watermark is an invisible identification code that as an integrated part of the design is permanently placed and any difference between the original data and the watermarked data does not exist. Watermark cannot be modified or deleted without damaging to the host. This paper present a solution based on RNS. We recommend use digital signature that the possibility of identity the recipient's right and author's right are preserved, based on multilevel- residue number system (RNS). This method is protecting a digital signature at the HDL design. That through a process of synthesis, replacement and routing is protected. This new technique enables high invulnerability.

2. Digital Watermarking

The information to be embedded in a signal is called a digital watermark. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

2.1 Applications

Old Methods of encrypting have not require efficient for obstruct unauthorized use and bad attacks from justified. In this condition exert data in form of invisible, has a high commercial potential. To overcome this problem, digital watermark has been raised. Digital Watermarking has variety of applications that the important of them are: broadcast monitoring, owner identification, proof of ownership, transaction tracking, authentication, copy control, device control, and legacy enhancement.

3. Residue Number System (RNS)

Residue number system is one of the display number systems. This system is an alternative to the traditional weighted numerical system, for applications that require fast mathematical operations of addition and multiplication. A residue number system by collection of modules as {P_1, P_2, P_3, $\ldots, P_n$} that all modules are defined positive integers. In this system, every number x is displayed by its residues of a set of modules. That causes the numbers of residue number system are smaller than commonly display and (So) Resulting in a smaller functional modules and the calculations are performed with greater speed and less power. Display the range of M is defined for a set of modules that obtained by multiplying all the modules together. A manner that is $M = \prod_{i=1}^{n} P_i$ .If the modules are the prime together, largest display range will calculated and can be sure that every number in the Residue number system of this range has a unique display. The Residue number system in applications such as digital signal processing, digital filters, and ... that require fast Calculations with low power consumption, is very convenient. This system with these features allows numbers break to smaller numbers without dependence on carry, in proper display that can be done Mathematical operations on

- *Sajjad Bagheri Baba Ahmadi is currently pursuing masters degree program in computer engineering in Cankaya University, Turkey, PH-00905432134601.*
- *E-mail: sajad_bagheri67@yahoo.com*
- *Yaser Ahangari Nanehkaran is currently pursuing masters degree program in information technology in Cankaya University, Turkey, PH-00905545058732.*
- *E-mail: y.ahangari@yahoo.com*

numbers in parallel and its top speed is use for such applications.

3.1 Select Modules in the Residue numbers System

Select a set of modules in the residue number system is an important factor, because style of select a set of modules that can shape a structure of residue number system. In general, the choice a set of modules that affects the simple circuit implementation of such modules, the maximum usage memory, ranges of exposure and complexity of mathematical algorithms. In select of set of modules, it should be attend that such choice of modules is better compared to prime together. Such a choice In addition to covers a huge range of numbers (according to the modules composition in a set) creates a unique collection for a binary number in the residue number system. During the last years many of researchers tried to offer a general form for set of modules that for difference amounts show always a set of modules which are primes together. In the next section we will examine some of the proposed modules.

3.2 Examine some of the proposed modules

Some of the modules, known modules, are used in the residue number system. In addition to make easy mathematic operates, combination them with other modules create a set of modules that members of them are prime together. For example can imply these modules $2^n, 2^n - 1, 2^n + 1, r^a, r^a - 1, r^a + 1$that r symbol is base of number. Some of proposed modules are defined by these following modules: $(2^n,\ 2^n + 1,\ 2^n - 1)$, $(2^n,\ 2^{n+1} - 1,\ 2^n - 1)$, $(3^n,\ 3^n - 1,\ 3^n - 2)$ and etc. These modules are prime together, by mathematical theorems such as Euclid’s theorem that used in this case is proved.

Theorem No.1

Tow numbers $2^b - 1$ and $2^a - 1$ are prime together if a, b are prime together and vice versa. In residue number system with m modules $\{2^{a_{m-2}} - 1,\ 2^{a_{m-1}} - 1, \dots, 2^{a_1} - 1,\ 2^{a_0} - 1\}$ that $a_{m-2} > \ldots > a_1 > a_0$ if $a_{m-2}, \dots, a_1\ , a_0$ are prime together. As a result, $2^{a_{m-2}} - 1, \dots, 2^{a_1} - 1, 2^{a_0} - 1$ are prime together.

Theorem No. 2 (Euclid)

If a, b are two integers, then we write: GCD (a, b) = GCD (a, b mod a). If this amount is equal to 1, so two numbers a, b are prime together.

Arithmetic operations and circuits of the residue number system

If supposed X, Y are two numbers in the residue number system Then generally arithmetic operations can be defined as following:

Z=X $\circ Y$

So we have:

$(z_1, z_2, \ldots, z_n) = (x_1, x_2, \dots, x_n) \circ (y_1, y_2, \ldots, y_n)$

If the set of modules used for these numbers are as $(m_0, m_1, \dots, m_n$)the result of operation will be as i= 1, 2, 3, … ,n , $z_i = (x_i \circ y_i)\ mod\, m_i$and the o operator can be addition, subtraction and multiplication. Division Operation can also be done in this system, but it is difficult. Otherwise in computation of computer used more operation addition. In next circuits we will offer adder circuit that has high computational speed. If suppose two numbers X, Y are residues of M module than $0 \le X \le m - 1, 0 \le Y \le m - 1$. For addition in M module firstly two numbers are added together, so the summation will be in range of $0 \le$X+Y$\le 2m - 2$. For to get the correct result ,in condition that summation of two number is greater than or equal to the module ,must subtract the size of module from summation of two numbers in according the following relation :

if Z=X+Y < m Then Z=X+Y

if Z=X+Y ≥ m Then Z=X+Y-m

3.3 Convert binary number system to RNS

For three known module $2^n - 1, 2^n$ and $2^n + 1$ converter algorithms and circuits are as follows. If a number in the binary number system, such as A with 2n digits and its remainder from it division on 2^n modulo, then we would have:

If the remainder obtained by dividing one number in the binary numeral system, such as A to 2^n -1, then we would be desirable:

$(\overbrace{a_{2n-1} \ldots a_{n+1}\ a_n}^{A_2}\ \overbrace{a_{n-1} \ldots a_1\ a_0}^{A_1})$ mod 2^n =

$[(\ a_{2n-1} \ldots\ a_{n+1}\ a_n) \times 2^n + (a_{n-1} \ldots\ a_1\ a_0)]$ mod 2^n =

$a_{n-1} \ldots\ a_1 a_0 =\ A_1$

$[(a_{2n-1} \ldots\ a_{n+1}\ a_n)\ \times (2^n - 1 + 1) +\ (a_{n-1} \ldots\ a_1 a_0)]\ mod\, (2^n - 1)\ =$

$(a_{2n-1} \ldots\ a_{n+1}\ a_n) + (a_{n-1} \ldots\ a_1 a_0)$

For obtain the remainder of division one number in binary system on 2^n -1 must n digits n digits of right apart and add together. If n digits of low weight called A1 and n digits of highest weight called A2, There is the possibility of creating three different modes for the summation:

$$A_1 +\ A_2 = \begin{cases} 0 \le\ A_1 +\ A_2\ <\ 2^n - 1 \\ 2^n - 1\ \le\ A_1 +\ A_2\ < 2(2^n - 1) \\ A_1 +\ A_2\ = 2(2^n - 1) \end{cases}$$

In fact the place value of I^{th} and $(i + jn)^{th}$ is equal. So when the sum of in the first relation is true because the value obatined is smaller than the module and the carry output is zero, then the summation is true and do not need to correction. But when the amount of summation in second and third relation is true, should subtract, as much as of the modules and twice size of the module, from summation respectively, or in the other hand as much as supplement of the above values (respectively one and two) are added to the summation. To increase speed, initially added require quantities and according to integer number is directed to output. The figure 1 can be used for this purpose.

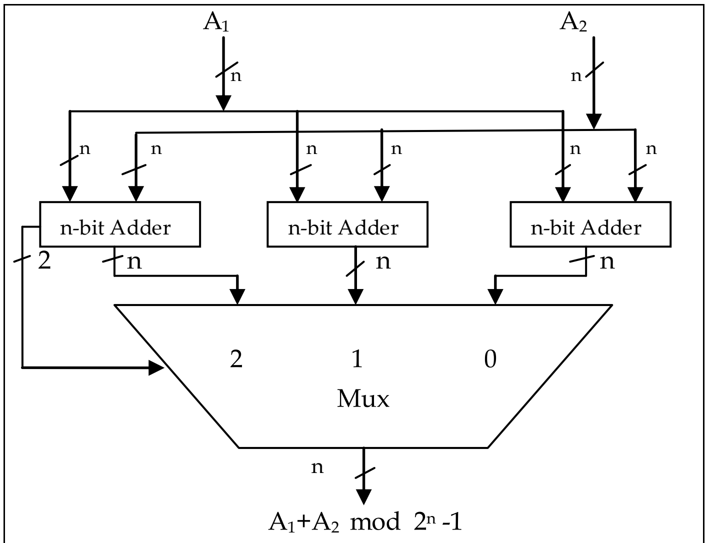

Figure 1.the circuit can be used of our purpose.

Finally, if we want to get the remainder of dividing one number (such as A in binary number system) and 2^n +1, then we will have:

$$(\overbrace{a_{2n-1}\ldots a_{n+1}\,a_n}^{A_2}\,\overbrace{a_{n-1}\ldots\,a_1a_0}^{A_1})\,mod\,(2^n+\ 1)=$$

$$[(a_{2n-1}\ldots\ a_{n+1}\ a_n)\ \times\ 2^n+(a_{n-1}\ldots\ a_1\ a_0)]\,mod\,(2^n+\ 1)=$$

$$[(a_{2n-1}\ldots\ a_{n+1}\ a_n)\ \times(\ 2^n+1-1)+$$
$$(a_{n-1}\ldots\ a_1\ a_0)]\,mod\,(2^n+\ 1)=$$

$$[-(a_{2n-1}\ldots\ a_{n+1}a_n)+(a_{n-1}\ldots\ a_1a_0)]$$

Consequently, for this purpose, should n digits n digits apart and subtract high weight digits from low weight digits. The place value of (i + n)th is minuse place value of Ith, thus the value of carry output digit is negative the value of carry input digit.

3.3. A Convert binary number system to two levels RNS

For convert binary number system to two levels RNS there are two ways direct and indirect. In indirect way, first number gets to RNS1 then residues of RNS1 get to RNS2. A sample of general diagram of convert binary number system to two levels RNS is shown in this paper as following figure 2:

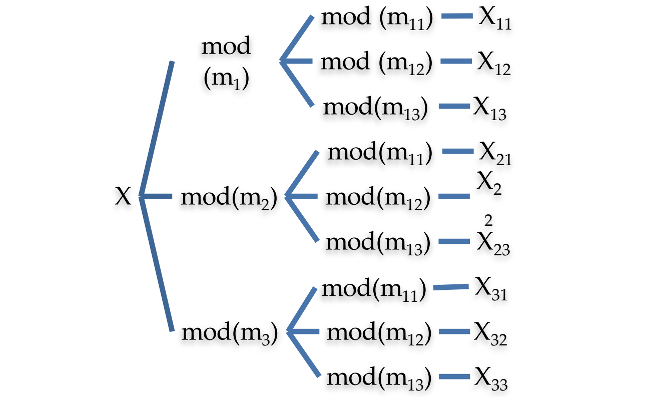

Figure 2. indirectly convert binary number system to two levels RNS

In inverse convert it require to three CRT numbers. For convert residues of second level to residues of first level and then by one CRT create the proposed weighter number. The binary number directly gets to RNS2 that according to results this way has more speed and low power. The generally idea of directly convert binary number system to two levels RNS is shown in following figure 3:

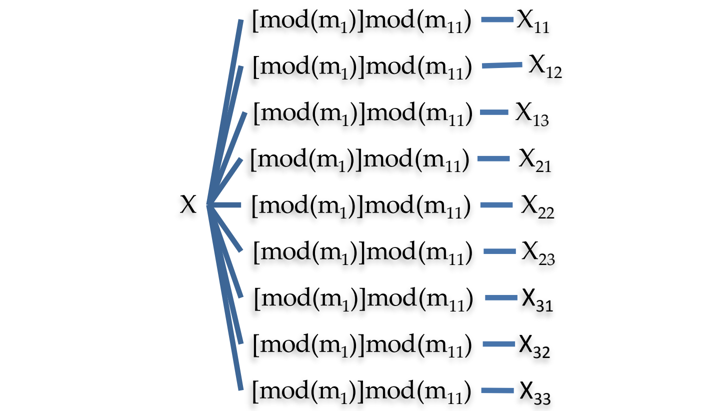

Figure 3. directly convert binary number system to two levels RNS

3.4 Convert RNS to binary number system

Convert residue number system to binary number is a process that in which a number as X = ($x_n, x_{n-1}, \ldots, x_0$) is shown to a unique number in binary system and define in the M range. For perform this conversion that it known as inverse conversion. There are a few methods: one of them is Chinese residue. It was the oldest methods used in mathematics. That is used in this part and can always be used in all modules in the residue number system. This method is the most comprehensive method to do a reverse conversion. To obtain number X of the residues of $(x_1, x_2, \ldots, x_n)$by Chinese residue theorem as the following procedure:

$$X=\langle\sum_{i=1}^{n}(x_i\ \times\ N_i)_{m_i}\ \times\ M_i\rangle_M$$

M = $\prod_{i=1}^{n} m_i$

$M_i=\ \frac{M}{m_i}, N_i=\ \langle {M_i}^{-1}\rangle_{m_i}$, i= 1, 2,…, n

That symbol $\langle {M_i}^{-1}\rangle_{m_i}$ is defined as inverse multiplication of Mi to a mi module. Generally inverse conversion circuit is also called N-Channel CRT. For calculate $(x_i\ \times\ N_i)_{m_i}$, first multiplied $(x_i\ \times\ N_i)$ by normal multiplier, then to obtain it's residue to proposed module by conversions which in the previous description, is very easy to do. In other hand these calculation do not require any new hardware.

4. Summary and conclusion

Watermarking technique is a suitable proposed by adding a digital signature protected in order to support the property rights based on RNS .This type of protection is available at the HDL design level and digital signature embedded in un-use positions of look-up tables of based on RNS. The embedded signature through a process of Conversion and data combination is transferred. That provides to enable efficient property rights based on RNS. Also the plan of extract signature by one another hardware in order increase resistance to attacks.

5. Suggestion

Watermarking is creating a secret identification in text, audio and video files, and creating these secret identifications will provide a reliable method for expert users for protecting copyrighted works, prove ownership, detect changes which made in images, databases and secretive communication. Our suggestion is that to generate code that we want to watermark. First make them by multilevel RNS. If the attacker wants to gained this code and destroy ownership right, first he/she must have numbers conversion module, second he/she must find all residues generated in the system be used. If he/she cannot find even one of the remaining numbers identify the number used in the RNS system is very difficult and almost impossible.

References

[1] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker "Digital Watermarking and Steganography, Second Edition" Elsevier publisher,2008.

[2] A.B Kahng, J.Lach,W. H Mangione-Smith,S.Mantik,I.L.Markov,M.Potkonjak,P.Tucker,H.Wang,G.Wolfe:constraint-Based Watermarking Techniques for design IP Protection,IEEE Transactions on computer-Aided computer-Aided design 1236-52,2001.

[3] L. Zhang, A. Li, "Robust watermarking scheme based on singular value of decomposition in DWT domain," in Proc.Asia-Pacific Conf. Information Processing (APCIP '09),vol. 2, Shenzhen, July 2009, pp. 19-22.

[4] Z. Shang, H. Ren, J. Zhang, "A block location scra mbling algorithm of digital image based on Arnold transformation," in Proc. 9th Int.Conf. Young Computer Scientists (ICYCS '08), Hunan, 2008, pp. 2942-2947.

[5] X. Zhu, J. Zhao, H. Xu, "A digital watermarking algorithm and impleme-ntation based on improved SVD," inProc. 18th Int. ConfPattern Recognition (ICPR '06), vol. 3, Hong Kong, 2006, pp.651- 656.

[6] Z. Rui-mei, L. Hua, P. Hua-wei, H. Bo-ning, "A blindwater mar king algorithm based on DCT," in Proc. 2nd Int.Symp. IntelligentInformation Technology Appl-ication (IITA '08), vol. 3, Shanghai, Dec. 2008, pp. 821 -824.

[7] E. Yavuz, Z. Telatar, "Improved SVD -DWT based digital image watermarking against watermark ambiguity,"in Proc. ACM symp.

[8] Alexander Skavantzos and Mohammad Abdallah, Member, IEEE "Implementation Issues of the Two-Level Residue Number System with Pairs of Conjugate Moduli" IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 47, NO.3, MARCH 1999.

[9] H. M. Yassine, "Hierachical Residue number system suitable for VLSI Arithmetic Architectures" IEEE, 1992.