International Journal of Intelligent Information Systems
2021; 10(3): 31-36
http://www.sciencepublishinggroup.com/j/ijiis
doi: 10.11648/j.ijiis.20211003.12
ISSN: 2328-7675 (Print); ISSN: 2328-7683 (Online)

Novel Access Control Mechanism Based New Chinese Remainder Theorem II (New Crt II)

Aremu Idris Aremu[1], Ibitoye Akinfola Akinrinnola[1], Nwaocha Vivian Ogochukwu[2]

[1]Computer Science Department, School of Technology, Lagos State Polytechnic, Ikorodu, Lagos, Nigeria

[2]Computer Science Department, Faculty of Science, Nigeria Open University, Ikorodu, Lagos, Nigeria

Email address:
aremu.i@mylaspotech.edu.ng (A. I. Aremu), mideeanddee@hotmail.com (I. A. Akinrinnola)

To cite this article:
Aremu Idris Aremu, Ibitoye Akinfola Akinrinnola, Nwaocha Vivian Ogochukwu. Novel Access Control Mechanism Based New Chinese Remainder Theorem II (New Crt II).*International Journal of Intelligent Information Systems*. Vol. 10, No. 3, 2021, pp. 31-36.
doi: 10.11648/j.ijiis.20211003.12

Received: March 17, 2021; **Accepted**: March 29, 2021; **Published**: June 22, 2021

Abstract: Security is a very vital concern in information system in this modern day. The protection of confidential files and integrity of information kept in the database are also of great important, the security model play an important role in protecting the privacy and integrity of messages in the database from unlawful users is a formal method to verify and describe intricate information system. An access Control mechanism is a main strategy for prevention and protection of the classified files in a database; this is carried out by restricting rights of access for different approved users of these files. This paper proposes a novel access control mechanism based on Chinese remainder theorem II which implements a single-key-lock system to encrypt one key called a secret key which is used for both encryption and decryption in the electronic information system for accessing the database. The key to be used in the decryption process must be exchanged between the entities in communication using symmetric encryption for the users to have access to the database. This method represents flocks and keys which is highly efficient and proficient. Also, this implementation can be achieved using the Chinese remainder theorem which executes faster operations and enables simpler construction of keys and locks to be provide for user to have access to control.

Keywords: Access Control, Residue Number System (RNS), New Chinese Remainder Theorem II (New CRT II)

1. Introduction

Data can be allocated to different users in the database in a time sharing system at a different time. Thus, the major unease task is to maintain the content of the file in the database by the database system chic [1-3]. Information stored in the database need to be protected from being damage, change or distorted without been notice by the database chic. The system supervisor needs to guarantee each user of the database, the use of the database resources in conformity with the policies of the system administrators. Information newly generated can be distributed across an extensive network for many users in the database environment; the safety of independent data becomes a heightened concern [4]. Cloud computing allows data sharing amid distinctive users of the database, which can be achieved with various degree of receptive means. As a result, controlling access system and stout isolation would be required.

Information fortification can be accomplished by means of an access control method. Once demand is made to access a file, it is interrupted by the control system to check for the validation before access can be given to the user [5]. The emergence of multimedia knowledge and distributed systems, has introduced the sharing of digital information across distinct users in unambiguous system or institution. These include video duplicates or digital audio, personnel data, commercial specifications, and digital books, which is stored in a universal database. Digital files are tremendously useful and must be confidentially reserved; to safeguard the content of the files from illegal access is a focus of eminent attention in the discipline of information security. The security of files during information accessing, is determined by an access control system employed to permit or hinder the access rights of distinct authorized users, i.e., to determine the degree of access distinct users have to the classified digital files. Therefore, the intrinsic purpose of the access control system is to avoid an unapproved users from viewing modifying and

damaging the digital files [6].

Therefore, an access control mechanism is a technology to secure the privileged files stored in a database by limiting the access rights of distinct authorized users of the files. [6].

An access control method is an assembly of components and methods that decide the order of admission by rightful users to activities determined by predefined access authorization and privileges defined in the access security strategy [7]. The elementary objective of this access control method is to regulate the user privileges and secure information from illegitimate access [8].

The residue number system (RNS) is a number system for representing integers which is capable of supporting parallel, high-speed arithmetic. This system also presents some valuable properties for error detection, error correction, and fault tolerance. It has several applications in computation-intensive digital signal processing (DSP) operations, like Fast Fourier Transform,, Discrete Fourier Transform, direct digital frequency synthesis, digital filtering, convolution, correlation etc [9].

Addition, subtraction, and multiplication, are arithmetic operations that can be performed independently and parallel in various residue channels more effectively than in the conventional binary systems. The adoption of RNS has offered notably effective improvements for distinct types of DSP applications [10].

2. Data Conversion

The forward conversion can be express as the execution of a forward converter which decomposes a weighted binary number into a residue represented number with regards to a moduli set, this implies the conversion from a conventional representation to a residue one by dividing the number X by each of the identified moduli and then collect their remainder [11]. For instance, given moduli set {3, 4, 5}, the number 4 can be represented in RNS as:

$$x_i = |X|_{m_i} \dots\dots \quad (1)$$

$$x_1 = |X|_{m_1} = |4|_3 = 1;\ x_2 = |X|_{m_2} = |4|_4 = 0; x_3 = |X|_{m_3} = |4|_5 = 4$$

Thus, the RNS representation of 4 is$(1, 0, 4)_{RNS(3,4,5)}$.

The basic technique in converting binary to RNS was presented by [11, 12].

New CRTII: To determine the correct decimal representation of the RNS number X with residue representation (x_1 , x_2 , $\dots x_n$) with respect to $\{m_1, m_2, m_3, , m_4\}$is

$$\text{X}=x_1 + m_1 \left| k_1(x_2\text{-}x_1)+k_2m_1(x_3 - x_2)+k_3m_1m_2(x_4\text{-}x_3) \right|_{m_2m_3m_4} \quad (2)$$

The difference between CRT II and the CRT is noticeable. CRT II does not have big modulo operations as compare to CRT, New CRTII is bounded by size $\sqrt{M}$ [13].

Illustration:

Given that $\{m_1, m_2, m_3, , m_4\}$are set of relatively co-prime number such that gcd(m_1, m_2)=1, gcd(m_1, m_3)=1, gcd(m_1, m_4)=1, gcd(m_2, m_3)=1, gcd(m_2, m_4)=1, gcd(m_3, m_4)=1. The decimal equivalent of residue representation of $\{x_1,x_2,x_3, x_4\}$ of an integer X is given as

$$\text{X}=x_1 + m_1 \left| k_1(x_2\text{-}x_1)+k_2m_1(x_3 - x_2)+k_3m_1m_2(x_4\text{-}x_3) \right|_{m_2m_3m_4} \quad (3)$$

such that

$$\left| k_1m_1 \right|_{m_2m_3m_4}\text{=1} \quad (4)$$

$$\left| k_2m_1m_2 \right|_{m_3m_4}\text{=1} \quad (5)$$

$$\left| k_3m_1m_2m_3 \right|_{m_4}\text{=1} \quad (6)$$

Given the set of 4moduli set of $m_1 = 2^n - 1$,m_2=$2^n + 1$,$m_3 = 2^{2n+1}$-1. By applying divide and conquer techniques we have two different sets of moduli i.e first moduli set= $\{m_1, m_2\}$ and second moduli set = $\{m_3, m_4\}$, we determine the decimal equivalent of first residue set$\{x_1,x_2\}$ and second residue set$\{x_3, x_4\}$. New Chinese remainder theorem can be used to compute for X_{12} and X_{34} as follows.

$X_{12} = x_1 + m_1 \left| k_1 (x_2 \text{-} x_1) \right|_{m_2}$ =first residue w.r.t first moduli set

$X_{34} = x_3 + m_3 \left| k_2 (x_4 \text{-} x_3) \right|_{m_4}$ =second residue w.r.t second moduli set

By merging it together i.e. merge $\{ X_{12} , X_{34} \}$ w.r.t $\{m_1, m_2,m_3, m_4\}$,

$$\text{X}=X_{12}+m_1m_2 \left| k_3(X_{34}\text{-}X_{12}) \right|_{m_3,m_4} \quad (7)$$

Demonstrating example:

$$\text{X}=(1,2,3,4)_{RNS(3,5,7,11)}$$

$$X_{12} = x_1 + m_1 \left| k_1(x_2\text{-}x_1) \right|_{m_2} \quad (8)$$

$$x_1 = 1\ m_1 = 3m_2\text{=5}$$

$$\left| k_1m_1 \right|_{m_2}\text{=1=} \left| 3^{-1} \right|_5\text{=2}$$

$$1\text{+3} \left| 2(2\text{-}1) \right|_5\text{=} \left| \left| 2 \right|_5\text{+} \left| \text{-1} \right|_5 \right|_5$$

$$1\text{+3(2) =7}$$

$$X_{34} = x_3 + m_3 \left| k_2(x_4\text{-}x_3) \right|_{m_4} \quad (9)$$

$$x_3 = 3\ m_3\text{=7 ,}\ m_4\text{=11}\ x_4 = 4$$

$$\left| k_1m_3 \right|_{m_4}\text{=1=} \left| 7^{-1} \right|_{11}\text{=8}$$

$$X_{34} = 3 + 7\left|8(4-3)\right|_{11}$$

3+7*8=59

3. Proposed Scheme

Given a moduli set $\{m_1, m_2, m_3, m_4\}$, its equivalent weighted number X can be transformed from the residue representation $(x_1, x_2, x_3, x_4)$by the definition of Divide and Conquer Techniques we have as follows:

$$X_{12} = x_1 + m_1|k_1(x_2 - x_1)|_{m_2} \tag{10}$$

$$X_{34} = x_3 + m_3|k_2(x_4 - x_3)|_{m_4} \tag{11}$$

Such that

$$|k_1 m_1|_{m_2} = 1$$

$$|k_2 m_3|_{m_4} = 1$$

$$X = X_{12} + m_1 m_2|k_3(X_{34} - X_{12})|_{m_3 m_4} \tag{12}$$

And also,

$$|k_3 m_1 m_2|_{m_3 m_4} = 1$$

Theorem 1:

Given $\{2^n - 1, 2^n + 1, 2^{2n}, 2^{2n+1} - 1\}$ moduli sets, by the definition of divide and conquer techniques, $m_1 = 2^{2n+1} - 1, m_2 = 2^{2n}, m_3 = 2^n + 1, m_4 = 2^n - 1$ then, we have $\{m_1, m_2\} and \{m_3 m_4\}$ and by definition of $|k_1 m_1|_{m_2} = 1$ and $|k_2 m_3|_{m_4} = 1$ the following hold true:

$$k_1 = 1$$

$$k_2 = 2^{n-1}$$

$$k_3 = 1$$

Proof:

If it can be demonstrated that $2^{2n+1} - 1$ with respect to 2^{2n} : $\left|2^{2n+1} - 1\right|_{2^{2n}+1} = 1$, then 1 is the multiplicative inverse of $2^{2n+1} - 1$ with respect to 2^{2n}. Similarly, $2^n + 1$with respect to $2^n - 1$: $\left|2^n + 1 \times 2^{n-1}\right|_{2^n - 1} = 1$, then 2^{n-1} is the multiplicative inverse of $2^n + 1$ with respect to $2^n - 1$. And also, $2^{2n-1} - 1 \times 2^{2n}$ with respect to $2^n + 1 \times 2^n - 1$: $\left|2^{2n-1} - 1 \times 2^{2n} \times 1\right|_{2^n + 1 \times 2^n - 1} = 1$, then 1 is the multiplicative inverse of $2^{2n+1} - 1 \times 2^{2n}$ with respect to $2^n + 1 \times 2^n - 1$.

By the definition of $X_{12} = x_1 + m_1|k_1(x_2 - x_1)|_{m_2}$ and $X_{34} = x_3 + m_3|k_2(x_4 - x_3)|_{m_4}$ we have

$$\begin{aligned} X_{12} &= x_1 + 2^{2n+1} - 1\left|(x_2 - x_1)\right|_{2^{2n}} \\ X_{34} &= x_3 + 2^n + 1\left|2^{n-1}\left(x_4 - x^3\right)\right|2^n - 1 \end{aligned} \tag{13}$$

And also by the definition of $X = X_{12} + m_1 m_2|k_3(X_{34} - X_{12})|_{m_3 m_4}$ we have

$$X = X_{12} + 2^{2n+1} - 1 \times 2^{2n}\left|X_{34} - X_{12}\right|_{2^{2n}-1}$$

Therefore the hardware realization of the proposed scheme will base on the following equations which can be further simplified as follow respectively:

$$\begin{aligned} X_{12} &= x_1 + m_1\left|(x_2 - x_1)\right|_{2^{2n}} \\ X_{34} &= x_3 + m_3\left|2^{n-1}\left(x_4 - x^3\right)\right|2^n - 1 \\ X &= X_{12} + 2^{2n+1} - 1 \times 2^{2n}\left|X_{34} - X_{12}\right|_{2^{2n}-1} \end{aligned}$$

$$\begin{aligned} X_{12} &= A \\ X_{34} &= B \\ X &= C \end{aligned}$$

Where

$$\begin{aligned} A &= x_1 + T \\ B &= x_3 + U \\ C &= X_{34} + V \end{aligned} \tag{14}$$

$$x_1 = \overbrace{x_{12n-1}x_{12n-2}x_{12n-3}\ldots\ldots\ldots\ldots x_{11}x_{10}}^{2n+1}$$

$$x_2 = \overbrace{x_{22n-1}x_{22n-2}x_{22n-3}\ldots\ldots\ldots\ldots x_{21}x_{20}}^{2n}$$

$$x_3 = \underbrace{00\ldots\ldots00}_{n}\overbrace{x_{3n}x_{3n-1}x_{3n-2}\ldots\ldots\ldots\ldots x_{31}x_{30}}^{n+1}$$

$$x_4 = \underbrace{00\ldots\ldots00}_{n}\overbrace{x_{4n-1}x_{4n-2}x_{4n-3}\ldots\ldots\ldots\ldots x_{41}x_0}^{n-1}$$

$$A = \overbrace{x_{12n-1}x_{12n-2}x_{12n-3}\ldots\ldots\ldots x_{11}x_{10}}^{2n+1} + \overbrace{11\ldots\ldots11}^{2n+1}\left|\overbrace{x_{22n-1}x_{22n-2}x_{22n-3}\ldots\ldots\ldots x_{21}x_{20}}^{2n} + \overbrace{\bar{x}_{12n-1}\bar{x}_{12n-2}x_{12n-3}\ldots\ldots\ldots x_{11}x_{10}}^{2n+1}\right|_{2^{2n}}$$

$$B = \underbrace{00\ldots00}_{n}\overbrace{x_{3n}x_{3n-1}x_{3n-2}\ldots\ldots x_{31}x_{30}}^{n+1} + \underbrace{00\ldots\ldots00}_{n+1}\left|\overbrace{11\ldots\ldots11}^{n-1}x(\underbrace{00\ldots00}_{n}\overbrace{x_{4n-1}x_{4n-2}x_{4n-3}\ldots\ldots x_{41}x_0}^{n-1} + \underbrace{11\ldots11}_{n}\overbrace{\bar{x}_{3n}\bar{x}_{3n-1}\bar{x}_{3n-2}\ldots\ldots\bar{x}_{31}\bar{x}_{30}}^{n+1}\right|_{2^n-1}$$

$x_1, x_2, x_3 and x_4\ 2^{2n+1}-1$

$$C = X_{12} + \overbrace{11\ldots\ldots\ldots11}^{4n+1}\left|X_{34} - X_{12}\right|_{2^{2n}-1}$$

We begin by explaining the component of the outcome from the New CRT II method, which is based on A, B and C. As it can be seen from equation 13 A, B and C are generated by Carry Save Adders (CSAs) with end around carries (EACs) taking the values x_1, x_2, x_3 and x_4. These values must be added modulo $2^{2n+1}-1$ in order to derive A, i.e., with a one's complement adder, namely a Carry Propagate Adder (CPA) with EAC. Bits easily derived by concatenating the operand x with the n-bit left shift of A. This concatenation does not require any additional hardware. The operands B required 2n bit which concatenation of m_3 which does not required any additional hardware also. And finally, C required 2n-1 bits moduli adder and also concatenation last three and four moduli of the set.

Forward conversion in the $\{2^n-1, 2^n+1, 2^{2n}, 2^{2n+1}-1\}$ moduli sets is straightforward and simple logic circuits, involving moduli adders, will suffice for implementation. If we define, $m_1 = 2^n+1, m_2 = 2^n-1, m_3 = 2^{2n}, m_4 = 2^{2n+1}-1$, then any integer X within the dynamic range $M = [0, 2^{6n+1} - 2^{4n+1} - 2^{4n} + 2^{2n} - 1]$ where upper and of the range is $(m_1 m_2 m_3 m_4)$ is uniquely defined by a residue set $(x_1, x_2, x_3 x_4)$, where $x_i = \left|X\right|_{m_i}$ and X is 6n+1 – bits:

$$X = x_{4_{2n}}x_{4_{2n-1}}\ldots\ldots\ldots x_{3_{2n-1}}x_{3_{2n-2}}\ldots\ldots\ldots x_{2_{n-2}}x_{2_{n-3}}\ldots\ldots\ldots x_{1_n}x_{1_{n-1}}\ldots\ldots x_0$$

Residue are obtained by nominally dividing X by m_i, the residue x_3 is the easiest to compute. The 2n least significant bits constitute the remainder when X is divided by the least significant 2n bits of X. these bits are obtained by nominally shifting to the right by 2n bits.

$$X_{12} = x_1 + m_1\left|\left(x_2 - x_1\right)\right|_{2^{2n}}$$

$$X_{34} = x_3 + m_3\left|2^{n-1}\left(x_4 - x^3\right)\right|2^n - 1$$

$$X = X_{12} + 2^{2n+1} - 1 \times 2^{2n}\left|X_{34} - X_{12}\right|_{2^{2n}-1}$$

Normally, because the shift may be hardwired. In order to determine the residues $(x_1, x_2, x_3 x_4)$ we first partition X into four 2n-bit blocks $B_1, B_2, B_3 and B_4$.

$$B_1 = \sum_{j=4n}^{6n+1} x_j 2^{j-4n}$$

$$B_2 = \sum_{j=2n}^{4n} x_j 2^{j-2n} \tag{15}$$

$$B_3 = \sum_{j=n}^{2n} x_j 2^{j-n} \tag{16}$$

$$B_3 = \sum_{j=0}^{n} x_j 2^j \tag{17}$$

Then,

$$X = B_1 2^{4n} + B_2 2^{2n} + B_3 + B_4 \tag{18}$$

The residue x_1 is obtained as

$$x_1 = \left|X\right|_{2^n+1} = \left|B_1 2^{4n} + B_2 2^{2n} + B_3 + B_4\right|_{2^n+1} \tag{19}$$

$$x_1 = \left|B_1 + B_2 + B_3 + B_4\right|_{2^n+1} \tag{20}$$

$$x_2 = \left|X\right|_{2^n-1} = \left|B_1 2^{4n} + B_2 2^{2n} + B_3 + B_4\right|_{2^n-1}$$

$$x_2 = \left|B_1 + B_2 + B_3 + B_4\right|_{2^n-1} \tag{21}$$

$$x_4 = \left|X\right|_{2^{2n+1}-1} = \left|B_1 2^{4n} + B_2 2^{2n} + B_3 + B_4\right|_{2^{2n+1}-1}$$

$$x_4 = \left|B_1 + B_2 + B_3 + B_4\right|_{2^{2n+1}-1} \tag{22}$$

4. An Application of New Chinese Remainder Theorem II to Access Control Method

The information protection system is employed to secure the access right of the information saved in the computer [14].

Table 1. *Access Control information.*

FILES / USERS	F_1	F_2	F_3	F4
U_1	3	0	2	2
U_2	2	0	2	0
U_3	0	2	0	1
U_4	4	1	1	2

0: No access 1: Executing 2: Reading 3: Writing 4: Owning.

Table 1, above shows an access control with four user and files, where U_i and F_i are denoted as user i and j, for users and files respectively.

First, the system assigns four relatively prime locks $L_1 = 10, L_2 = 17, L_3 = 21\ and\ L_4 = 15$ to the files $F_1, F_2, F_3\ and\ F_4$ respectively. These lock to control by the access rights for each file. Then, the system computes four keys by using forward conversion $K_1, K_2, K_3\ and\ K_4$ by New CRT II for the four users$U_1, U_2, U_3\ and\ U_4$, respectively.

5. Performance Analysis

This segment considers some issues about the proposed access control methods, as well asthe computational complexity related with the construction of the keys and the storage requirement for the keys and locks. The implementation of the proposed mechanism is based on below equation.

$$X_{12} = x_1 + m_1 \left|(x_2 - x_1)\right|_{2^{2n}}$$

$$X_{34} = x_3 + m_3 \left|2^{n-1}\left(x_4 - x^3\right)\right| 2^n - 1$$

$$X = X_{12} + 2^{2n+1} - 1 \times 2^{2n} \left|X_{34} - X_{12}\right|_{2^{2n}-1}$$

Assume that $\{m_1 m_2, \ldots . m_n\}$ are set of moduli set of relatively co-prime integer called moduli sets, with residue representation of $\{x_1, x_2, \ldots . x_n\}$ where the GCD(m_i,m_j)=1. The New CRT II for moduli set that are relatively co-prime needs to compute the equation $X_{12} = x_1 + m_1 \left|(x_2 - x_1)\right|_{2^{2n}}$ $X_{34} = x_3 + m_3 \left|2^{n-1}\left(x_4 - x^3\right)\right| 2^n - 1$ such that $X = X_{12} + 2^{2n+1} - 1 \times 2^{2n} \left|X_{34} - X_{12}\right|_{2^{2n}-1}$ $X_{12} = x_1 + m_1 \left|(x_2 - x_1)\right|_{2^{2n}}$ with constant time complexity i.e 0(1), $X_{34} = x_3 + m_3 \left|2^{n-1}\left(x_4 - x^3\right)\right| 2^n - 1$ with constant time complexity i.e. 0(1), which has to do with n-bit 1's complement operation and $X = X_{12} + 2^{2n+1} - 1 \times 2^{2n} \left|X_{34} - X_{12}\right|_{2^{2n}-1}$ it required 0(logn) and the hardware complexity are n-bit 1's complement operation and n-bit multiplication and n-bit 1's complement operation. The proposed scheme required 0(logn) for the time complexity and five n-bit for the hardware (area) complexity.

Table 2. *Hardware Computation Complexity comparison.*

Mechanisms	Method	Time Complexity	Storage Requirement
[1] mechanism	GCRT	0($n^2\ b^2$)	0(m+n)
[6] mechanism	GART	0(nb^2)	0(m+n)
Our proposed mechanism	CRT11	0(logn)	0(logm+n)

So, 0(log m + n) form keys and n locks thus avoiding the overflow problem.

6. Conclusion

The efficient access control method proposed is predicated on the concept of the single key lock method, based on forward conversion and Chinese remainder theorem II (CRTII) for both key and lock respectively. The proposed method utilized an effective technique to produce keys for users. First, choosing n pairwise co-prime integers L_j for 1 ≤ j ≤ n as the keys of the n files and determing the access right a_{ij} of distinct user U_i to each digital file F_j in the invisible access control matrix. The key K_i for distinct user U_i can be generated easily by the locks, $L_1, L_2, \ldots . L_n$, U_i's rights CRTII. We examined the time complexity of the CRTII and determined that the method are more efficient than [1].

References

[1] D. E. Derming and P. J. Denning, "Data Security," ACM Comp. Survey, Vol. 1 No. 3, (1979), pp 227-249.

[2] B. W. Lampson 'Protection" *Proc. 5th Princeton Sytnp. of Info. Sci. and Syst., Princeton* Univ., (1971), pp. 437-443.

[3] G. S. Graharn and P. L. Denning, "protection-principles and practice," *Proc. Spring Jt. Computer Coference,* Vol. 40, AFIPS Press, Montvale, N. J., (1972), pp. 417-29.

[4] Kim S. Lee et al. A Hierarchical Single-Key-Lock Access Control Using the Chinese Remainder Theorem. ACM 1992.

[5] Baumann, A., Peinado, M., & Hunt, G. (2015). Shielding applications from an untrusted cloud with haven. *ACM Transactions on Computer Systems (TOCS)*, *33* (3), 1-26.

[6] M. L. Wu, T. Y. Hwang, Access control with single-key-lock, IEEE Trans. Software Eng. 10 (2) (1994) 185-191.

[7] Yanjun Liu, Chin-Chen, and Shih-Chang Chang, An Access Control Mechanism Based on the Generalized Aryabhata Remainder Theorem. *International Journal of Network Security, Vol. 16, No. 1, PP. 58-64, Jan. 2014.*

[8] Anderson R. Security Engineering: a guide to building dependable distributed systems. John Wiley & Sons; 2010. p. 640.

[9] Younis A. Younis, KashifKifayat, MadjidMerabti. An access control model for cloud computing. journal of information security and aplications 19 (2014) 45-60. Elsevier Ltd.

[10] Vilardy, J. M., Giacometto, F., Torres, C. O., & Mattos, L. (2011, January). Design and implementation in VHDL code of the two-dimensional fast Fourier transform for frequency filtering, convolution and correlation operations. In *Journal of Physics-Conference Series* (Vol. 274, No. 1, p. 012048).

[11] Ouyang, J., Coatrieux, G., & Shu, H. (2015). Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform. *Digital Signal Processing*, *41*, 98-109.

[12] Chervyakov, N. I., Molahosseini, A. S., Lyakhov, P. A., Babenko, M. G., & Deryabin, M. A. (2017). Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem. *International journal of computer mathematics*, *94* (9), 1833-1849.

[13] C. H., Premkumar, A. B., & Zhang, W. (2013). A new RNS based DA approach for inner product computation. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *60* (8), 2139-2152. Omondi A. and Premkumar B (2007): Residue Number Systems: Theory and Implementation. Imperial College Press, 2007.

[14] Ouye, M. M., & Crocker, S. T. (2018). *U.S. Patent No. 10,033,700*. Washington, DC: U.S. Patent and Trademark Office.