

A New Chinese Remainder Algorithm for Image-based Encryption

Sergio Duarte[†], David Becerra[†], Yoan Pinzón[†]

Fecha de Recibido: 09/06/2008 Fecha de Aprobación: 01/02/2009

Abstract

In this paper, a novel method for image encryption based on a Generalized Chinese Remainder Theorem (GCRT) is presented. The proposed method is based on the work developed by Jagannathan *et al.* Some modifications are proposed in order to increase the method's encryption quality and its robustness against attacks. Specifically, the inclusion of a vector to reduce the segment pixel space and a Generalized Chinese Remainder Theorem (GCRT) algorithm are proposed. These vectors are generated randomly which allows its use as private keys joining these unrestricted key values generated by the GCRT algorithm. An analysis to study a system where the RGB channels are independently encrypted is performed. Some experiments were carried out to validate the proposed model obtaining very promising results.

Keywords: *Image Encryption, Chinese Remainder Theorem, Algorithms, Information Security.*

[†] Grupo de Investigación en Algoritmos y Combinatoria (ALGOS-UN), Universidad Nacional de Colombia, Bogotá, Colombia, {srduartet,dcbecerraypinzon}@unal.edu.co

[‡] Se concede autorización para copiar gratuitamente parte o todo el material publicado en la *Revista Colombiana de Computación* siempre y cuando las copias no sean usadas para fines comerciales, y que se especifique que la copia se realiza con el consentimiento de la *Revista Colombiana de Computación*.

1 Introduction

Images represent a very important source of information in many science and technology areas. The intensive use of this kind of information has grown in an exponential way over the last decades as a consequence of the Internet's explosion and the development of hardware to manipulate multimedia information. This growth brings the urgent need to develop newer and more efficient mechanisms to protect the multimedia material given the intrinsic risk of their transmission over a media as the Internet [2].

Information security has become a very important topic given the sensibility and confidentiality of information transmitted as images. In previous approaches, the encrypting processes have been performed applying techniques such as the discrete cosine transform DCT [6], the Fractional Fourier Transform (FRFT) [4], information theory and entropy [7] and some recent variations of the chaotic key-based algorithm (CKBA) [8] have been proposed too.

In this paper, a novel image encryption scheme is proposed, mainly based on the use of modular arithmetic over the model developed by Jagannathan *et al.* [1] in which the CRT algorithm is used on JPG images. This method performs a compression on an encrypted image, which is proper given the high cost of image transmission in a remote way. An inherent advantage of the proposed method is its highly adaptability to different security environments, because contrary to other methods based on DCT [9] it does not depend on previous processing and compression technologies. Additionally, this method overcomes some limitations of selective image encryption methods, where some improvements over the running time are obtained at expense of encryption security ruggedness.

This paper is structured in the following manner. Section 2 contains a brief description of the state-of-the-art in image encryption methods. A mathematical background necessary to understand the CRT method is given in Section 3. In Section 4, some generalized approaches to the CRT method are studied along with a detailed description of the proposed Generalized Chinese Remainder Theorem (GCRT). In Section 5, an application of the GCRT to encrypt and compress images is explained. Subsequently, an experimental framework and its results are discussed. Finally, some conclusions are drawn together in the final section.

2 Encrypted Image Methods

Cryptography makes reference to the set of mathematical and algorithmic techniques applied to guard information's confidentiality. Cryptography methods must keep the inherent features of a security system as the authenticity (which refers to the ability of unambiguously distinguish the receiver), the integrity (which refers to the inability to modify a message without being detected) and the non-repudiation property (which is a way to prove that a given sender actually sent a particular message) [9].

Image encryption methods depend on the scenario where they are performed. The scenario features include the infrastructure on which the system is implemented (software or hardware); the sort of access to the data to be encrypted (partial or total) and, finally, if there is information loss in the encryption process (lossy or loseless). These features determine the algorithms which could perform complete or partial encryption, key generation can be symmetric or asymmetric and the information processing can be in blocks or sequential [11].

In a complete encryption method all the bytes of an image are encrypted followed immediately by a compression process. On the contrary, the selective encryption processes use *a priori* information from the compression method and from the data structures which were used to encrypt the most relevant information. Although these methods are more efficient with respect to the required time in the encryption process, they are less robust from a security point of view than a complete encryption algorithm [9]. The selective methods are popular given their suitability to be applied in communication systems as in the internet where the transmission time and the storage space are a high priority.

Even if the proposed method could be applied in different scenarios given that it is a method of complete encryption, the encryption process using CRT is a symmetric encryption method because it generates only one set of keys that is used by the sender and receiver. Additionally, this method uses a data block which enables its parallelization. In the following section we will outline the main mathematical concepts used in the proposed encryption system.

3 Chinese Remainder Theorem (CRT)

The original CRT could be found in a book dating back to the III century A.C., written by the Chinese mathematician Sun Tzu [12, 13], it was

republished in 1247 by Qin Jiushao. Despite its age it is still an extremely useful and necessary tool in information security and it has lots of good applications such as in codification, cryptography, and signal processing [14], to name some.

Such theorem is based on a linear congruence system and it could be formulated in the following way. We want to find an x , given the residues a_1, a_2, \dots, a_k which were obtained dividing by n_1, n_2, \dots, n_k , then a set of linear congruencies should be solved.

A congruence equation is an equation like:

$$f(x) \equiv b \pmod{n} \quad (1)$$

Where the values $0 \leq x \leq n$ are searched. This kind of equations could have none, one or many solutions. Solving equation (1) consists of finding all the integers x that satisfy the following equation.

$$ax + my = b \quad (2)$$

Two or more linear congruences could be solved using the CRT algorithm. m and n should be any two positive integers,

$$x \equiv a \pmod{m} \quad (3)$$

$$x \equiv b \pmod{n} \quad (4)$$

Two linear congruences will be solvable when

$$a \equiv b \pmod{\gcd(m, n)} \quad (5)$$

And the solution will be the unique module (least common multiple) $\text{LCM}(a, b)$.

In equation (5) when m and n are *coprimes*, its *greatest common divisor* is equal to one and by convention $a \equiv b \pmod{1}$ is conserved for any a and b .

A congruent module could be defined as:

$$a \equiv b \pmod{n} \quad \text{iff} \quad \begin{cases} n \mid (a - b) \\ a \bmod n = b \bmod n \end{cases} \quad (6)$$

The CRT could be defined in the following way [3]. Let n_1, n_2, \dots, n_k be integers and pairwise relatively prime. If a_1, a_2, \dots, a_k are arbitrary integers, the system of simultaneous congruences (7) has a unique solution module $N=n_1n_2\dots n_k$ given by (8).

$$x \equiv a_i \pmod{n_i} \quad \forall_i \in \{1 \dots k\} \quad (7)$$

$$x = \sum_{i=1}^k N_i y_i a_i \pmod{N} \quad (8)$$

Where $N_i = N/n_i$ and $y_i = N_i^{-1} \pmod{n_i}$.

The algorithm that implements the equations described above could be enclosed in time complexity $O(k \log(n))$.

In this paper, we formalize the Generalized Chinese Remainder Theorem and propose an algorithm to solve it. This algorithm will find the shortest positive integer that satisfies a congruence system and the period in which these solutions are repeated (in case that more than one solution exists). The algorithm will also work whenever integers m and n are not coprimes. This algorithm will be central to the proposed image encryption scheme because it will allow the selection of keys in a domain bigger than $[0 \dots 255]$. Hence, it guarantees that the method will still work even if the divisors are randomly taken from 1 to 16, and overcoming some of the limitation shown in [1] where the divisor should be a constant equal to 16.

4 A Generalized Chinese Remainder Theorem.

The method developed by Ore [15] and the method of successive substitutions have been reported to solve the problem of restrictive modules in the definition of the CRT. The successive substitution method is based on practical applications of the congruence equations. On the other hand, the Ore method is based on an extended terminology of the CRT and concludes that the solution for a congruence system without module restrictions could be presented as follows (c.f. [15] for a formal proof of this).

$$x \equiv a_1 c_1 \frac{M}{m_1} + \dots + a_k c_k \frac{M}{m_k} \pmod{M} \quad (9)$$

where the c_i form a set of integers that satisfies the following condition.

$$c_1 \frac{M}{m_1} + \dots + c_k \frac{M}{m_k} = 1 \quad (10)$$

4.1 The proposed Generalized Chinese Remainder Theorem.

```

1      Begin GCRT
2      If (The modules are coprimes) then
3          Use CRT;
4      Else
5          Initialization();
6          Use GCRT();
7      End if
8      End GCRT
9      Begin GCRT
10     While Not all the equations were evaluated do
11         Find LCM();
12         Find the greatest no coprime integer;
13     End while
14     Find the new  $a_i$ ;
15     Build a new equation system;
16     Use CRT();
17 End CRT General

```

Fig. 1. Pseudo-code for the proposed GCRT

The proposed approach is based on the basic idea to process any congruence system using the traditional CRT (see Fig 1). If the equation set does not meet the restrictions (no coprimes) to be solved by the traditional CRT method, then the algorithm should convert it to a new set of equations, where it would be possible to use the traditional CRT. In the proposed approach an initial calculation of the period over the new system should be performed.

In line 5 (see Fig. 1), the function computes the Least Common Multiple between all the modules in the system. The function GCRT computes the new congruence system that satisfies the constraints of the traditional CRT, and guarantees that this system should provide a solution set to the original equation system. In other words, there should exist a transformation between both systems, where the unique solution for the system (the transformed one) that meets all the constraints should be a solution of the systems that does not satisfy those constraints.

The general idea is to evaluate all the congruences in order to find the greatest non-relatively prime and the least multiple of the non-coprimes

modules. The time complexity for performing this process is $O(n)$, where n is the number of equations.

The computation of LCM for the non-relatively primes is performed as a division of the total LCM computed in the function *Initialization* by each one of the found modules that are non-relative primes between them. This value will correspond to the n_k and it is interpreted as the module in the new equation system.

The computation to find the greatest non-relatively prime is important because it is used to find the new a_i for the new transformed system. Additionally, this computation decreases the number of comparisons needed to find this new system. In line 14 the operation to find a new a_k is performed a number of times according to the result of the division between the LCM and the highest non-relatively prime. As the while loop progresses, some shift of length equal to the size of the highest found module is performed. This is done in order to find the a_k that meets all the equations that are actually transformed. Note that, it is not necessary to evaluate all the possible options for a_k , instead only those values where the a_k are feasible for the highest found module are evaluated, so only those equations where the modules are non-relative primes should be evaluated.

Having the n_k and a_k , it is possible to build the new equation system. This new system which fits the traditional CRT constraints is now handled as a classical CRT problem. It is important to note that the solution given by this system corresponds to the first (smallest) solution of many solutions that could have the congruence systems with non- relatively primes. The solutions of this system will be repeated for a period equal to the LCM of the set of equations evaluated with the traditional CRT.

5 Image Encryption Scheme Using GCRT.

In the proposed approach, as in the method given in [1], the image is represented using a matrix of size $2^n \times 2^n$. Additionally, the analyzed images are codified with the JPEG standard. This standard was chosen given its extended acceptance and popularity, but the proposed algorithms could be easily applied to other formats.

For color images, a three channel (RGB model) representation will be used. This implies that in the encryption process three matrices with

same size are built, one for each channel. In computational terms, each position contains a data of eight bits whose values are in the interval $[0, 255]$. For each one of these matrices, it is necessary to apply the encryption and recuperation processes described in the following sections.

5.1 Image Encryption

From an image of size $N \times N$ pixels a segmentation process, where each block has size K , is performed. Each one of the pixels in the segment is divided by a set of random divisors chosen from the interval $[1, 16]$ ($i = [p_1, p_2, p_3, \dots, p_k]$). The set of divisors (common for all the segments) is $d = [d_1, d_2, d_3, \dots, d_k]$. The residue vector for the congruencies is $a = [p_1/d_1, p_2/d_2, p_3/d_3, \dots, p_k/d_k]$, and the equation set is $x = a_i \pmod{n_i} \forall i \in \{1, 2, \dots, k\}$ where the set $n = [n_1, n_2, n_3, \dots, n_k]$ represents the keys for the encryption system, contrary to the proposed method in [1] where for each segment element a different divisor (which was randomly selected), was computed.

Although a divisor ensures a steady decline in regular bits representation of the pixels, build a vector of random divisors (vector d) improves the quality of encryption because it is less susceptible to attacks and the variability of the encrypted image over the original is greater. Moreover, thanks to the proposed GCRT, the constraints to get random divisor which could not be coprimes is overcome. Additionally, this concept could be extended to apply a vector d_c of divisors independently to each channel, and then we will have two matrixes of keys with size $K \times 3$ for the encryption system.

Next the equation system is solved using equation (8). It is important to note that the values N_i and y_i are common to all the pixels in the image, and then it is possible to preprocess these values to increase the efficiency of the approach. Given that the k pixels of a segment are presented through a unique value, this methodology leads to a decrease in the space required to represent the encrypted image. Specifically, the compression factor in bits with this approach is:

$$c = \frac{1}{8K} \quad (11)$$

As a result, when the segmentation and CRT process are applied, the resulting encrypted image is represented by a matrix of size $N \times K$. This matrix will be referred as the matrix E from now onwards.

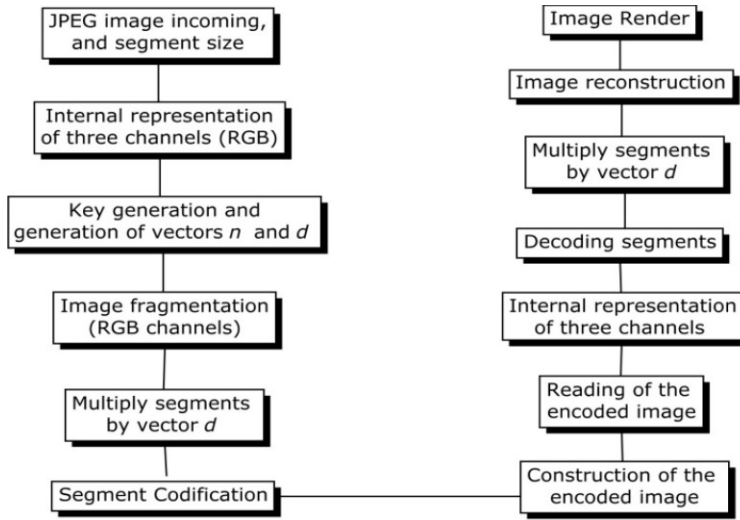


Fig. 2. Flow chart of the encryption scheme

5.2 Decryption of the Image

The image is reconstructed by applying to each element of the encrypted matrix the following equation:

$$a_i = X_{h,j} \bmod(n_i) \quad \forall i \in \{1, 2, \dots, K\} \quad (12)$$

where $X_{h,j}$ belongs to the matrix $E_{N \times K}$, which was obtained in the encryption process. For each $X_{h,j}$ the K pixels are recovered without information loss. Once the values a_i are calculated, they are multiplied by the elements in the vector d :

$$r_i = a_i \times d_i \quad \forall i \in \{1, 2, \dots, K\} \quad (13)$$

The image originally encrypted is recovered by applying equations (19) and (20) to all the segments. The procedure is identical in the case of having a different vector d for each channel being processed.

In Fig. 2 a flow chart of the main process in the scheme is depicted. Initially, the image to process is entered to the system and the parameter k of the segment is determined. Then each one of the image channels is processed using a matrix. The channel α which corresponds to the image

transparency is not taken into account for a simplified procedure. Next the keys (vector n) are randomly generated in order to apply the GCRT and the divisor vector is generated too. Three variants were used to generate the key vector, the first consists of using the predefined value for all the elements in n , the second consists of using random values for each one of the values in the vector n . Finally, the generation of random values for independent divisor vectors of each channel was explored. The motivation to perform the second and third options was to increase the encryption security and the data dispersion of the encoded image, *i.e.*, how the original image differs from the encoded image. In the next step the image segmentation is performed, specifically, for each pixel in the segment, a division over the corresponding component in the vector d (as it was described in Section 4.1) is computed.

Once the divisor elements have been applied to all the segments, the GCRT algorithm is performed, thus the k pixels are represented in the segment by a value X , getting compression and encryption at the same time. The same process is repeated for all the segments (in total N^2/k segments). Next, the coded image of size $N \times K$ is built and it is stored in a JPG format.

The reverse process is similar, where for each element in the encrypted matrix, k pixels are obtained through the equations described in Section 4.2. Then for each reconstructed segment its elements are multiplied by elements of the vector d . Finally, the image is reconstructed given that the previous process was done over the three matrixes that codified the RGB channels.

6 Experimental Framework and Results.

The image encryption scheme was applied to a JPG image (*Lena*) of size 256x256 pixels and the values PSNR (*Peak signal to noise ratio*) was found for different configurations of the encryption keys. This value is a similarity measure between both images and it is computed as the difference in pixels between the original and the encoded image. This measure is generally used to quantify the loss of quality in the image compression. If this measure is approaching to infinity then the two images are equal and if the measure is zero both images are completely different [4].

$$MSE = \frac{1}{MN} \sum_{y=1}^M \sum_{x=1}^N [I(x, y) - I'(x, y)]^2 \quad (14)$$

$$PSNR = 20 * \log(255 / \sqrt{MSE}) \text{ (8-bit value).}$$

The main motivation is to contrast the sensibility of the application by introducing different wrong keys, both for the vector n as for the vector d .

Some results obtained by the proposed scheme using the *Lena* image and a size segment equal to four are shown in *Table 1*. In the first column the outcome images after applying the same value d_i for the entire components in vector d are shown. In the second column different random values for each component in the vector d were taken. In the third column, a vector of different keys for each channel and other with the same values for all the components in vector d are used. Finally, for the last column independent vectors of different keys for each channel and independent vectors of random divisors were used.

In the first row the image recovered by the system applying the correct keys is shown, in the second row the result of decoding the image using three correct keys and one false is shown. In the third row the result using two correct keys and two wrong keys is shown and so on. For the second column two different values in the vector d were established. Finally, in the fourth column the results for two different values for each of the divisor vectors corresponding to each channel are shown. Additionally, Fig. 3 shows the display generated by the application of the encrypted image. Note that the image is not square as a result of the segmentation that takes place in the encryption process.

Table 2 shows the obtained measures from PSNR and RMS for images that are in the first two columns in Table 1. The result shows that the tolerance to attacks by the second column is significantly higher than in the first, because even if a subset of keys is discovered the decrypted image greatly differs from the original. In addition, while the keys are found, there is not a marked progression in the similarity of the decrypted image over the original. This fact has a great significance because it hinders the work of decoding the image when there is not a full knowledge of the keys, since it makes more difficult to detect when a correct key has been found. Contrary to the images belonging to the first column where it is clear that while the number of correct keys increase, the image rapidly converges to the original image. Likewise, the knowledge of three correct keys for the second column does not imply a substantial similarity with the original image. Finally, it is important to notice that the decrypted image with the whole set of correct keys are not





















Decryption with a single constant value for the vector d	Decryption with random values for the vector d	Decryption with matrix keys and a single value for d	Decryption with matrix keys and matrix divisors
			
			
			
			
			

Table 1: Decryption results



Fig.2 . Visualization of the encoded image.

exactly equal to the original image. This phenomenon is easily explainable given that the channel α which corresponds to the image

transparency was not taken into account, although the noise level is quite low. Table 3 shows the RMS and PSNR measures for the third and fourth column of Table 1, where an independent key vector for each channel was used.

When the same value for all divisors is kept it could be seen that the similarity between the decrypted image and the original one increases significantly as the keys are discovered, which is an undesirable behavior in an encryption system. But the encryption has better quality compared to the approach applied in the first column since the dispersion between the images is higher.

When vectors of divisors were generated randomly and independently for each channel, an improvement in the behavior of the system could be observed, since even if only one key is wrong, significant differences between the decrypted and original images are obtained. Additionally, there is not a clear trend in the similarity of both images while the keys of the system are discovered.

Wrong keys	Measure	Single value to d	Random d vector
0	RMS	5.3	
	PSNR	32,9	
1	RMS	44.53	88.25
	PSNR	15.15	9.21
2	RMS	59.3	94.75
	PSNR	12.68	8.59
3	RMS	81.67	100.07
	PSNR	9.88	8.12
4	RMS	84.77	111.38
	PSNR	9.56	7.19

Table 2: Quantitative encryption results using single constant and random values in vector d .

Wrong keys	Measure	Single value to d	Random Matrix d
0	RMS	4.9	
	PSNR	34,1	
1	RMS	54.92	107.12
	PSNR	13.35	7.53
2	RMS	79.38	99.13
	PSNR	10.13	8.2
3	RMS	88.62	105.07
	PSNR	9.1	7.7
4	RMS	113	112.15
	PSNR	7	7.13

Table 3: Quantitative encryption results using an independent key vector for each channel with constant values in d and a divisor matrix

7. Conclusions and Future Work

Based on the experimental results, it is possible to conclude that the proposed GCRT is a feasible and efficient method for image encryption. [However, the selection of keys in a domain greater than $[0, 255]$ increases the degree of security in the system, the encrypted image would have a bigger size in bytes than the original. Therefore if a

specific level of compression is wanted, shorter keys should be chosen decreasing the level of security.

A significant improvement is obtained by using a vector of divisors

instead of a constant value as it was set out in [1]. This technique improves the encryption quality (understood as the divergence of the image by applying incorrect keys) and the system security, making the approach more tolerable to attacks.

However, it was further noted that the utilization of key vectors, for each channel of the image, improves the quality of the encryption but not its behavior against attacks.

The inclusion of independent divisor vectors to the model significantly improved the behavior of the system. These results confirm the importance of using different random divisors in the encryption method.

A new Generalized Chinese Remainder Theorem was proposed to solve any equation system of congruencies, where the algorithmic complexity, the validation of the solutions and guarantees the existence of a solution (with its period) are some of the advantages of this method with respect to the state of the art.

Additionally, the method is based on an intuitive and basic idea that makes the method easy to understand. Note that the proposed algorithm has all the theoretical advantages given by the classical CRT.

The proposed algorithm expands the search space of keys in encryption methods that use CRT. Specifically, the proposed encryption scheme benefits from GCRT, given that it allows the key selection over bigger domains overcoming the inherited limitations of the classic CRT.

In future work, it is important to extend the application to allow processing images of arbitrary size. Regarding the encryption method, it is important to consider the influence of the segment size over the encryption quality and feasibility in order to get lower and upper levels of these parameters.

References

- [1] Vikram Jagannathan, R. Hariharan, Aparna Mahadevan and E.Srinivasan, Number theory based image compression encryption and application to image multiplexing. **IEEE Signal**

Processing, Communications and Networking, International conference, pp. 56-64, 2007.

- [2] S.Wong, L. Zaremba, D. Gooden, and H. K. Huang, Feb. Radiologic Image Compression-A review, Proc. IEEE, vol. 83, pp. 194–219, 1995.
- [3] Lin, K.-Y.; Krishna, B.; Krishna, H. **Rings, fields, the Chinese remainder theorem and an extension-Part I: theory.** IEEE Transactions on [see also Circuits and Systems II: Express Briefs, IEEE Transactions on] Volume 41, Issue 10, pp. 641 – 655, 1994.
- [4] George P. Mulopulos, Laszlo S. Gasztonyi, Albert A. Hernandez, Peak Signal to Noise Ratio Performance Comparison of JPEG and JPEG 2000 for Various Medical Image Modalities. Symposium on Computer Applications, 2003.
- [5] G. Unnikrishnan and Kehar Singh. Double random fractional bourier-domain encoding for optical security. *Optical engineering*, 39(11)pp.2853–2859, 2000.
- [6] L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In *Proceedings of the ACM Multimedia 1996*, pp 219–229, 1996.
- [7] Chung-Ping Wu and C.-C. Jay Kuo. Fast encryption methods for audiovisual data confidentiality. In *SPIE Photonics East - Symposium on Voice, Video, and Data Communications*, volume 4209, pp 284–295, 2000.
- [8] Daniel Socek, **Shujun Li**, Spyros S. Magliveras and Borko Furht, **Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption.** In *Proceedings of the First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005)*, pp. 406-408, 2005.
- [9] Andreas Uhl, Andreas Pommer. Image and Video Encryption From Digital Rights Management to Secured Personal Communication, In *Advances in Information Security*, Springer, 2005.
- [10] Chung-Ping Wu and C.-C. Jay Kuo. Efficient multimedia encryption via entropy codec design. In *Proceedings of SPIE, Security and Watermarking of Multimedia Contents III*, San Jose, CA, USA, volume 4314, 2001.
- [11] Xiliang Lu and Ahmet M. Eskicioglu. Selective encryption of multimedia content in distribution networks: Challenges and new directions. In *Proceedings of the IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003)*, Scottsdale, AZ, USA, 2003.
- [12] L.E. Dickson. History of the theory of numbers. Vol. II:

- Diophantine analysis. Chelsea Publishing Co., New York, 1966.
- [13] Kang Sheng Shen. Historical development of the Chinese remainder theorem. Arch. Hist. Exact Sci., 38(4): pp 285-305, 1988.
 - [14] C. Ding, D. Pei, and A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Coding and Cryptography. World Scientific Publishing, 1997.
 - [15] O. Ore, The General Chinese Remainder Theorem, Yale University, The American Mathematical Monthly, Vol. 59, No. 6 pp. 365-370, July 1952.