International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.2, Mar-Apr 2012 pp-018-020 ISSN: 2249-6645

Enhanced RSA Combined with DWT Domain Watermarking

Saira Varghese [1], Leda Kamal[2]
*(Department of Computer Science, Toc H Institute of Science & Technology, India)
** (Department of Computer Science, Toc H Institute of Science & Technology, India)

ABSTRACT

This paper presents a framework of combining enhanced RSA algorithm with watermarking techniques for hiding secret information in digital images.RSA algorithm is one of the widely used public key algorithms. Considering increment of security requirements, size of the keys has been larger. With key length growing, delay of exponentiation computation has changed into major problem in selecting longer keys. With enhanced RSA cryptosystem, delay in exponentiation calculation is reduced substantially. Encryption and watermarking are two major tools that can be used to prevent unauthorized consumption and duplications. Enhanced RSA encrypted data and watermark is embedded inside an HSV (Hue Saturation Value) color image using Discrete Wavelet Transform (DWT) algorithm. The accuracy of the wavelet transform is determined after reconstruction by calculating the Mean Square Error (MSE), Correlation and Peak Signal to Noise Ratio (PSNR) of the signal. The invisible robust watermarking using DWT leave the original data unchanged. The original plain text can be obtained by applying enhanced RSA decryption algorithm over the extracted cipher text.

***Keywords* - DWT, HSV, RSA, Watermarking.**

1 INTRODUCTION

Information security is a fundamental requirement for an operational information society. Although issues considered as information security, such as secrecy of messages, privacy of communication, and reliable authentication, to name a few, have been important throughout history, developments in digital computing and information technology have set new requirements and challenges for them. The importance of information security has grown because new technologies have made accessing and misusing confidential information easier and more profitable.

Cryptography is defined as the science of using mathematics to encrypt and decrypt data that enables the storage and transmission of sensitive data in a secure manner. Cryptography has two processes; the first process is the encryption where the original data is converted into secured form using certain specified steps. The second process is the decryption, where the encrypted data is restored to the original form by applying the inverse to the steps applied in the encryption process. RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. Because of wide uses of networks during the last decade and growing security requirements in communication, public-key cryptosystems have been regarded highly. Nowadays choosing a key with 1024-bit length to apply in RSA is a good way to prevent analyses predictions, but in the near future 2048-bit and even 4096-bit key lengths will become available. Increasing number of multiplication operations is a problem that appears due to public-key growing and more operations means more delay in case of encryption and decryption in RSA. The modulo exponentiation in RSA has 2(k-1) multiplications in worst case and (k-1) multiplications in best case where k is the number of bits in key[1]. In this context an enhanced RSA algorithm is used to increase the speed of exponentiation operation.

Watermarking represents an efficient technology for ensuring data integrity and data-origin authenticity. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection algorithm [2][3].In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark. The literature survey explains robustness is the resistance of an embedded watermark against intentional attacks such as noise. DWT is any wavelet transform for which the wavelets are discretely sampled. As with others wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time) The Discrete Wavelet Transform (DWT), which is based on sub-band coding is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district [3][4]. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). Daubechies (db1)derives a family of wavelets, the first of which is the Haar wavelet. The db1 wavelet is same as Haar wavelet. The dwt2 performs single-level two-dimensional wavelet decomposition with respect to either a particular wavelet and computes the approximation coefficients matrix cA and details coefficients matrices cH, cV, and cD (horizontal, vertical, and diagonal, respectively).Single level inverse discrete 2D wavelet transform idwt2 performs a single-level two-dimensional wavelet reconstruction with respect to either a particular wavelet.

2 IMPROVED TECHNIQUES

2.1 Enhanced RSA Algorithm

The purpose of modular exponentiation is computing M^e mod (n) to achieve the result with the least multiplication operation and memory requirements. The classical method to do modular exponentiation is binary method or square-and-multiply method. In binary method, exponentiation result can be achieved by squaring or squaring and multiplying depended on exponent's bits. The binary algorithm calculates exponentiation with (k-1) to 2(k-1) multiplications according to Hamming weight of the exponent. To solve this problem, in improved exponentiation algorithm M^e mod (n) is considered as a collection of 2^l modular multiplications.ie squaring and multiplication is done in parallel. TABLE 1 presents the parallel computation[1]. The enhanced RSA algorithm uses this method for modular exponentiation.

Parallel Computation

Step	Squaring	Final Result(multiplication)

Initial	*M:= M mod n*	*If(e_0=1) then C:=M(mod n)*
		else C:=1

Parallel algorithm	*for j=1 to l*
	M_j:= M_{j-1}×M_{j-1}(mod n)
		for i=1 to l
		if(ei≠0)
		C:=C×M_i(mod n)

2.2 Embedding encryption in Watermarking

The data encrypted using enhanced RSA algorithm is used for watermarking. In DWT-based watermarking, the DWT coefficients are modified to embed the watermark data [3]. Because of the conflict between robustness and transparency, the modification at a given level is usually made in HL, LH, and HH sub-bands[3].To measure distortion and similarity between the original watermark (W) and the extracted watermark (W'), Peak Signal to Noise Ratio, Mean Square Error and Correlation are computed. These metrics will help the user decide if a watermark can be consistently recovered with the given method [5].

3 PROPOSED ALGORITHM

This paper proposes a new implementation of embedding enhanced RSA encrypted data in watermarking digital images. This architecture is presented using enhanced RSA algorithm and Discrete Wavelet Transform (DWT) for performing encryption and watermarking respectively.In watermarking Discrete Wavelet Transform(DWT) technique is used for achieving robustness.

3.1 Encryption and Watermark Embedding

1. Apply enhanced RSA encryption on plaintext to produce cipher text.
2. Read cover image and secret image.
3. Combine secret image and cipher text to generate the watermark.
4. Apply DWT on original image and watermark.
5. Add the watermark in original image using IDWT.

3.2 Watermark Distilling and Decryption

1. Obtain watermarked and encrypted image.
2. Recover watermark by taking the difference of watermarked and encrypted RGB image and the value part of HSV image.
3. Recover secret image by applying DWT.
4. Recover cover image by taking the difference between watermarked and encrypted RGB image and recovered watermark.
5. Recover cipher text from recovered watermark.
6. Calculate PSNR, MSE and Correlation Coefficient.
7. Apply enhanced RSA decryption to recover plaintext.

4 ANALYSIS

Nowadays choosing a key with 1024-bit length to apply in RSA is a good way to prevent analyses predictions, but in the near future 2048-bit and even 4096-bit key lengths will become available. Increasing number of multiplication operations is a problem that appears due to public-key growing and more operations means more delay in case of encryption and decryption in classical RSA.Enhanced RSA which uses improved exponentiation algorithm provides a solution to this problem.

The parameters such as Peak Signal to Noise Ratio (PSNR) for the host image, Correlation Coefficient (CC) and the Mean Square Error (MSE) for the watermark can be used to evaluate the performance of the watermarking technique used.

5 CONCLUSION

In this paper we have proposed a method for embedding encrypted messages in watermarked images. In the first phase encryption is performed using enhanced RSA algorithm and in the second phase watermarking is done using Discrete Wavelet Transform. This design combines the computational speed of enhanced RSA algorithm and robustness of DWT based watermarking technology. By combining these efficient techniques information security can be achieved. Peak Signal to Noise Ratio(PSNR),Correlation coefficient and Mean Square Error (MSE) metrics can be computed for the extracted watermark and the original watermark to examine the degree of distortion.

The proposed method grants the authenticity of the transmitted data, thanks to the watermarking technique, and the privacy, obtained through the encryption procedure.

Finally, the proposed method can be used for exchanging highly secret messages most likely for defense departments.

REFERENCES

[1] S.Sepahvandi, M. Hosseinzadeh and K. Navi and A.jalali "An Improved Exponentiation Algorithm for RSA Cryptosystem "*DOI 10.1109/ICRCCS, IEEE 2009.*

[2] Rawa I. Zaghloul,Enas F.Al-Rawashde..“HSV Image Watermarking Scheme Based on Visual Cryptography”, *Proceedings of World Academy of Science, Engineering and Technology 44, 2008.*

[3] Anumol T.J ,P Karthigaikumar, “DWT based Invisible Image Watermarking Algorithm for color Images,” IJCA Special Issue on *''Computational Science –New Dimensions and Prespectures,''NCCSE 2011,pp 76-79.*

[4] Mei Jiansheng,Li Suleang and Tan Xiaomei, “A Digital Watermarking Algorithm Based On DCT and DWT,” *in Proceedings of the 2009 International Symposium on Web Information Systems and Applications, May 2009,pp 104-107* .

[5] Emir Ganic ,Ahmet M Eskicioglu, “Robust DWT-SVD Domain Image Watermarking Embedding Data In All Frequencies,”*in Proceedings of MM&SEC'04,2004,pp 166~174.*