ISSN: 2321-7782 (Online)
Volume 2, Issue 8, August 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / SurveyPaper / Case Study
Available online at: www.ijarcsms.com

Digital Watermarking using Asymmetric Key Cryptography and Spatial Domain Technique

Krishna Kumar Singh[1]
Department of Computer Science & Engineering
United College of Engineering & Research
Allahabad, India

Shashank Dwivedi[2]
Department of Computer Science & Engineering
United College of Engineering & Research
Allahabad, India

Abstract: ***Earlier the digital watermarking was evaluated according to imperceptibility, capacity and robustness. In this paper based on security considerations we address a new secure approach. Our new approach is inspired from the cryptanalytic approach. In order to achieve higher secrecy and efficiency we use a combined approach based on both digital watermarking and Cryptography together for embedding the secret information. The purpose of our work is to enhance the security of secret information embedding into the cover image. We implement an asymmetric key cryptography technique (RSA) and spatial domain technique in digital watermarking.***

Keywords: Digital Watermarking, RSA, Spatial Domain, types of digital watermarking, Asymmetric Key Cryptography.

I. INTRODUCTION

Digital watermarking is a pattern of bits embed into digital multimedia content such as image, audio, video. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners [1]. The main difference between watermark and digital watermark is that digital watermark are supposed to be invisible or at least not changing the perception of original file whereas watermark are supposed to be somewhat visible. A signal may carry several different watermarks at the same time. If the signal is copied, then the information is also carried in the copy.

II. TYPES OF DIGITAL WATERMARKING

A. Based on Human Perception

It is sub-divided into two categories:

- ***Visible Watermarks***

  In visible watermarks, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

- ***Invisible Watermarks***

  In invisible watermarks, the information is not visible by the viewer. Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As the quality of image does not suffer much, it can be used in almost all the applications. [2]

B. Based on Applications

It is sub-divided into three categories:

- ***Fragile Watermarks***

  These watermarks are very sensitive. They can be destroyed easily with slight modification in the watermark signal.

- ***Semi-Fragile Watermarks***

  These watermarks are broken if the modification to the watermark signal exceed a predefined user threshold. If the threshold is set to zero, then it operates as a fragile watermark. This method can be used to ensure data integrity and also data authentication.

- ***Robust Watermarks***

  These watermarks cannot be broken easily as they withstand many signal processing attacks. Robust watermark should remain intact permanently embedded signal such that attempts to remove or destroy the robust watermark will degrade or even may destroy the quality of image. This method can be used ensure copyright protection of the signal.

C. Based on level of information required to detect the embedded data [Kejariwal (2003)]

It is sub-divided into three categories:

- ***Blind Watermarks***

  These watermarks detect the embedded information without the use of original signal. They are less robust to any attack on the signal.

- ***Semi-Blind Watermarks***

  These watermarks require some special information to detect the embedded data in the watermark signal.

- ***Non-Blind Watermarks***

  These watermarks require the original signal to detect the embedded information in the watermark signal. They are more robust to any attack on the signal when compare to blind watermarks.

D. Based on user's authorization to detect the watermark [Kejariwal (2003)]

It is sub-divided into two categories:

- ***Public Watermarks***

  In this watermarking, the user is authorized to detect the watermark embedded in the original signal.

- ***Private Watermarks***

  In this watermarking, the user is not authorized to detect the watermark embedded in the original signal.

E. Based on knowledge of the user on the presence of the watermark [Kejariwal (2003)]

It is sub-divided into two categories:

- ***Steganographic Watermarking***

  The user is not aware of the presence of the watermark.

- ***Non-Steganographic Watermarking***

  The user is aware of the presence of the watermark.

III. LITERATURE SURVEY

Asymmetric key cryptography is also known as public key cryptography, refers to a cryptographic algorithm which requires two separate keys one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext; whereas the private key is used to decrypt cipher text.

Asymmetric key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate his or her public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is "impossible" (computationally infeasible) for a properly generated private key to be determined from its corresponding public key. Thus the Asymmetric key may be published without compromising security, whereas the private key must not be revealed to anyone not authorized to read messages. Asymmetric key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of one (or more) secret keys between the parties [3].

RSA is normally considered as a strong asymmetric key cryptographic technique [4]. By taking this point into consideration, MoumitaSahaet. Al have worked on the development of a watermarking scheme involving RSA technique for the encryption of the watermark in 2007 [5].The objective of the work is to embed some copyright information (like company name, author, date of release, copy number, and any other relevant information) in the media file using steganography. The concepts of steganography and cryptography have been combined in the proposed approach. Steganography is used to hide the existence of information in the media file, and cryptography is used to encrypt the information before hiding. They used a keyed stream cipher architecture controlled by a key which is the product serial number to transform the hashed information before hiding. And finally, they used the RSA algorithm controlled by the private key of the origin to encrypt the cipher stream along with the product serial number and is hidden inside the media file.

It was proven that to achieve reasonable security, a 1024-bit modulus would have to be used in a RSA cryptosystem, while a 60-bit modulus is sufficient for ECC which started receiving commercial acceptance in the late 1990s [6].

IV. ALGORITHM

RSA (Rivest, Shamir and Adleman) is normally considered as a strong asymmetric key cryptographic technique. RSA is an algorithm for Asymmetric key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem.

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem.

RSA scheme is a block cipher which uses expression with exponentials. The key length is of variable size. Here, the cipher text size is depending on the key size. The detailed steps of the algorithm are given below:

Algorithm

1. Choose two large prime numbers p and q.
2. Calculate n = p * q and ϕ (n) = (p-1)*(q-1).
3. Choose an integer e, such that e is co- prime to ϕ (n).
4. Compute the secret d such that (d *e) mod ϕ (n) =1.

5. Now, the public key is (e, n) and private key is (d, n).

6. The sender can encrypt the message P as $C = P^e \bmod n$

7. The receiver can regenerate the message P as $P = C^d \bmod n$

As the computation of the secret d from public key (e, n) is quite difficult, this algorithm resists the common attacks. Hence, it is considered to be a secured algorithm.

RSA Algorithm Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute ϕ (n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < ϕ (n) and gcd(ϕ (n),e)=1. Let e = 7
- Compute a value for d such that

  $$(d * e) \bmod \phi(n) = 1$$

  One solution is d = 3 as

  $$(3 * 7) \bmod 20 = 1$$

- Public key is (e, n) = (7, 33)
- Private key is (d, n) = (3, 33)
- The encryption of m = 2 is

  $$c = 2^7 \bmod 33 = 29$$

- The decryption of c = 29 is

  $$m = 29^3 \bmod 33 = 2$$

V. WATERMARKING TECHNIQUE

Image watermarking techniques proposed so far can be divided into two groups according to the type of feature set the watermark is embedded in: spatial domain techniques (where watermarks are embedded in intensity values) and transform domain techniques (where watermarks are inserted in transform coefficients).

Spatial domain

The simplest way to embed a watermark in the spatial domain is to select a pseudo random set of pixels and to modify the Least Significant Bits (LSB) of their intensity values. In long m-sequences are added to the LSB of the images pixel intensities, and detection is performed by computing the spatial cross-correlation. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications. The drawbacks of spatial domain methods are that in general they are not robust to common geometric distortions and have a low resistance to JPEG compression; moreover, since the watermark casting algorithm can embed only few bits in the image to respect the requirement of unobtrusiveness, they seem to offer a low bit capacity.

Techniques in spatial domain class generally share the following characteristics:

1. The watermark is applied in the pixel domain.

2. No transforms are applied to the host signal during watermark embedding.

3. Combination with the host signal is based on simple operations, in the pixel domain.

4. The watermark can be detected by correlating the expected pattern with the received signal.

In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image.

The algorithm proposed by Kurah and McHughes [7] to embed in the LSB and it was known as image downgrading [3]. An example of the less predictable or less perceptible is Least Significant Bit insertion. The principle of embedding is fairly simple and effective. If we use a gray scale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a gray scale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colours between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each colour component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures [8]. For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal.

VI. IMPLEMENTATION

Embedding Scheme:

Algorithm:

1. Owner chooses two large prime numbers p and q.

2. Then, owner calculates the private key (d, n) and public key (e, n).

3. By using the public key, the owner encrypts the original image to produce Encrypted watermark image.

4. Embed the Encrypted watermark in the spatial domain of cover image and as a result Stego image is formed.

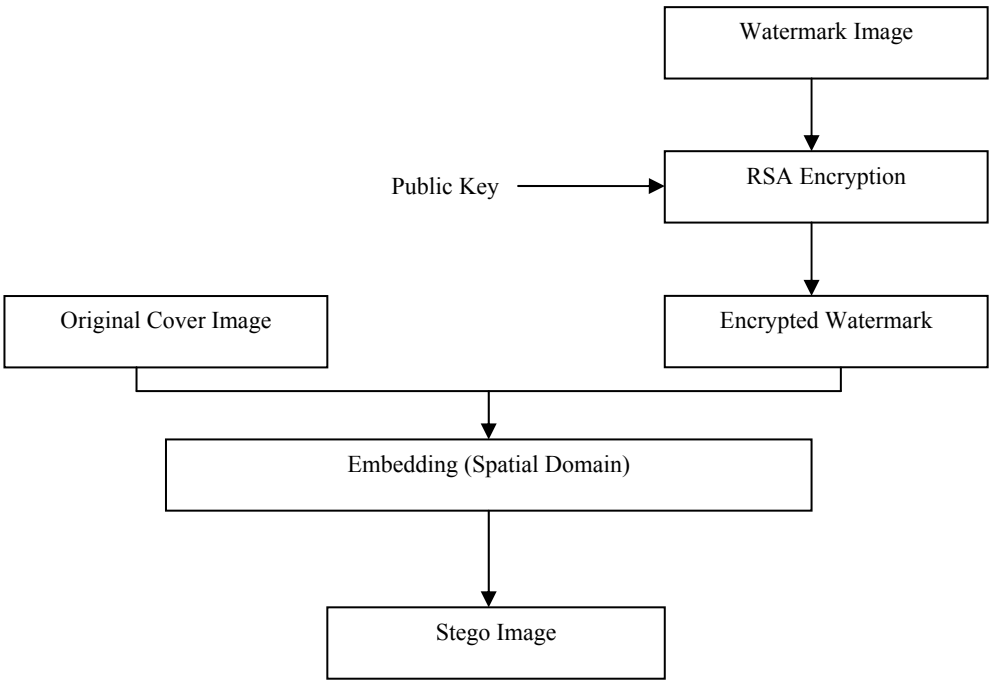

Fig. 1 Embedding Process

Extraction Scheme:

Algorithm:

1. The encrypted watermark is extracted from the Stego image (Spatial domain).

2. By using the private key, the owner decrypts the Encrypted watermark and as a result original watermark is recovered.

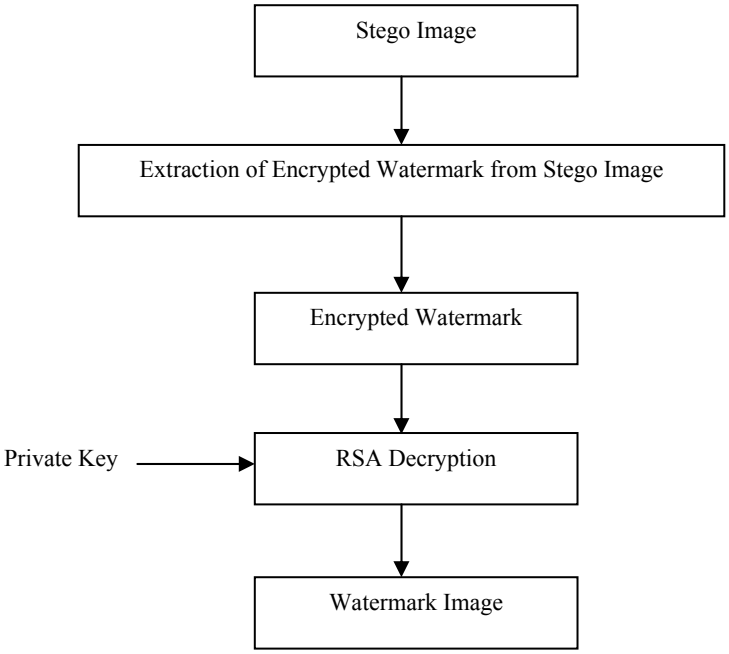

Fig. 2 Extraction Process

Results Analysis:

For the experimental results, we have taken lena64.bmp as the original image of size 64*64 as shown in Figure (a). The original image is encrypted by RSA technique with the owner's public key results RSA encrypted watermark image as shown in Figure (b). Similarly, baboon.bmp has been taken as the cover image of size 512*512 as shown in Figure (c). The embedded cover is shown in Figure (d). When the extraction process is applied to the embedded cover image, we have got the image as shown in Figure (e). After applying RSA decryption with owner's private key, the original image is recovered as shown in Figure (f).

Fig. (a) original Image

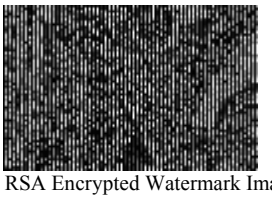

Fig.(b) RSA Encrypted Watermark Image

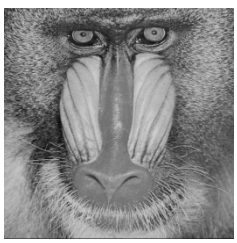

Fig. (c) Cover Image

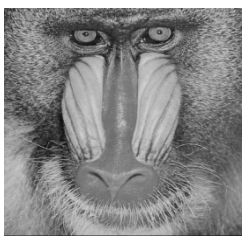

Fig. (d) Embedded Cover Image

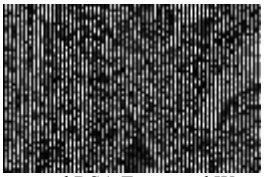

Fig. (e) Extracted RSA Encrypted Watermark Image

Fig. (f) Decrypted Original Image

Fig. 3 RSA Result Analysis

The metrics used to test the robustness of the algorithm are Peak Signal to Noise Ratio (PSNR), values are calculated considering the following images:


Fig. 4 lena.bmp

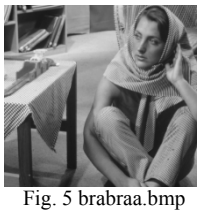
Fig. 5 brabraa.bmp

Table 1
PSNR Values

Image	PSNR
lena.bmp	+58.64dB
barbara.bmp	+58.99dB

VII. CONCLUSION

Cryptography in digital watermarking is the current area of research where lot of scope exists. Currently cryptographic technique in digital watermarking is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic cryptographic technique introduced till now.

This paper starts from some basic knowledge of digital watermarking, includes the classification of digital watermarking. We have started working on Asymmetric Key Cryptography and implementing the same in digital watermarking. In future course of study, the aim of this paper is to extend the asymmetric key cryptography to higher dimensions and apply it in transfer domain.

ACKNOWLEDGMENT

We are very thankful to the faculty of United College of Engineering & Research for giving us full freedom to access the lab facilities to carry out this work. We wish to thank our friends & family members for being patient with our many distractions and diversion during the completion of this work.

References

1. http://en.wikipedia.org/wiki/Digital_watermarking
2. Gaurav Chawla, Ravi Saini, Kamaldeep, Rajkumar Yadav, ”Classification of Watermarking Based upon Various Parameters”, International Journal of Computer Applications & Information Technology Vol. I, Issue II, September 2012, pp. 16-19.
3. Behrouzan A. Forouzan, "Cryptography and Network Security", TMH Publisher, 2010, ISBN. 9780070660465.
4. Moumita Saha, Monu Kedia, Indranil Sen Gupta, "A Robust Digital Watermarking Scheme for Media Files", TENCON, IEEE, November 2007 pp. 1-4.
5. Hongbin Kong, Zhengquan Zeng, Lijun Yan, Jicheng Yang, Shaowen Yao ,Nuoya Sheng, "Combine Elliptic Curve Cryptography with Digital Watermark for OWL- Based Ontology Encryption", IEEE International Conference on Computational Intelligence and Security, 2009, pp. 511-515.
6. Youssef Zaz, Lhoussain El Fadil, "Enhanced EPR Data Protection using Cryptography and Digital Watermarking", IEEE International Conference on Multimedia Computing and Systems, 2010, pp. 1-5.
7. Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang, Mengmeng Wang, "Digital Image Encryption Algorithm Based on Pixels", IEEE International Conference on Intelligent Computing and Intelligent Systems, 2010, pp. 769-772.
8. Siddharth Singh, Tanveer J Siddiqui, Rajiv Singh, Harsh Vikram Singh, "DCT-domain Robust Data Hiding Using Chaotic Sequence", IEEE International Conference on Multimedia, Signal Processing and Communication Technologies, 2011, pp. 300-303.

AUTHOR(S) PROFILE

Krishna Kumar Singh was born in Mirzapur, Uttar Pradesh, India in 1991. He received Bachelor Degree (B.Tech) in Information Technology, Aryabhatt College of Engineering and Technology, Baghpat, Gautam Buddha Technical University, Lucknow in 2012. He is pursuing Masters Degree (M.Tech) in Computer Science & Engineering from United College of Engineering and Research, Allahabad, Uttar Pradesh Technical University, Lucknow.

Shashank Dwivedi was born in Mizapur, Uttar Pradesh, India in 1972. He is Associate Professor and Head of Department of Information Technology at United College of Engineering and Research, Allahabad, India. He has teaching experience of 14 years. He did his Masters Degree (M.Tech) in Information Technology from Ram Rao Adik Institute of Technology, Mumbai University. His area of interest includes Computer Organization, Automata, Design and Analysis of Algorithm.