# Image Authentication System based on Digital Watermark and Digital Signature

Ei Shwe Sin Win, Myat Thida Mon
*University of Computer Studies, Pyay*
*shwesin13@gmail.com, myattmon@gmail.com*

## Abstract

*In this paper to protect copyright, ownership and content integrity of digital media including digital watermarking techniques. The primary motivation of this article is to study the principles of cryptographic primitives and watermarking schemes. In this paper, we propose a secure verification system for watermarked images with the intention of copyright protection. RSA algorithm, RSA signature, multi-signatures,, and LSB technique are employed in the proposed system. The proposed system is developed by C# programming language. This projected system can withstand compression brightness and no attack can destroy copyright of the image, in addition, no one can alter content of transmitted images. In this paper ,we use RSA multi -signature algorithm to protect unauthorized distribution and LSB technique to embed and detect watermark.*

## 1. Introduction

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data [1].

Digital watermarking is a technique used to protect the digital media property. Copyright is a form of intellectual property which gives the creator of an original work exclusive right for a certain time period in relation to that work, including its publication, distribution and adaptation [5].

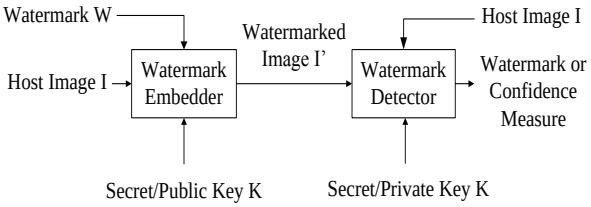



Fig-1: General model of watermarking systems

Digital watermarking is the process of possibly irreversibly embedding information into a digital signal. Visible watermarking is associated with the perception of the human eye to identify where the information has been embedded on the image. Invisible watermarking is the method that can hide the information on the image analyzing if invisible to the human eye.

In this paper, the proposed system applies RSA algorithm to get the confidentiality for watermark RSA multi-signature to protect unauthorized distribution RSA signature to prevent from malicious codes, and LSB technique to embed and detect watermark.

## 2. Related Works

Many multimedia documents are produced and distributed widely for many applications. And those many multimedia documents are spread fast through the Internet. And there have been illegal behavior that many unauthorized users transform a multimedia and use illegally so, legal issues for copyrighted multimedia arise as a necessary consequence.Digital watermarking recently emerged as an effective solution to these problems as it can preserve the copyright and data security [2]. Minerva M. Yeung and Fred Mintzer proposed a system which employed LSB technique intended for image verification [4]. The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels. The watermark is actually invisible to human eyes. However, the watermark can be easily

destroyed if the watermarked image is low-pass filtered or BMP compressed. To increase the security of the watermark, Matsui and Tanaka proposed a method that uses a secret key to select the locations where a watermark is embedded. Voyatzis and Pitas used a toral automorphism approach to scramble the digital watermark before a watermark is inserted into an image. In my proposed system, LSB technique is also applied as well as other cryptographic primitives to give the superlative security to the copyright and content of the watermarked image.

## 3. RSA Public Key Cryptosystem

In today's world of cryptography, the most widely known public key cryptographic system is RSA. A public key cryptographic system is a form of modern cryptography, which eliminates the use of a previously agreed upon shared secret key, allowing users to communicate securely with one another. General of public key cryptosystem is shown in Fig-2.

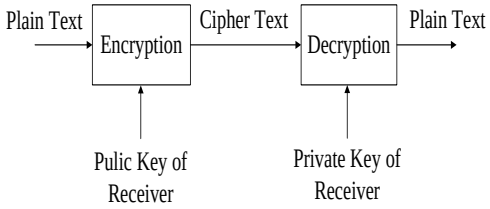



Fig-2: General model of public key cryptosystem

## 4. RSA Multi-signature

A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document. RSA multi-signature allows two entities to sign a message which can be validated by another entity. In order to multi-sign the message $M$ RSA multi-signature scheme is as follows [6].

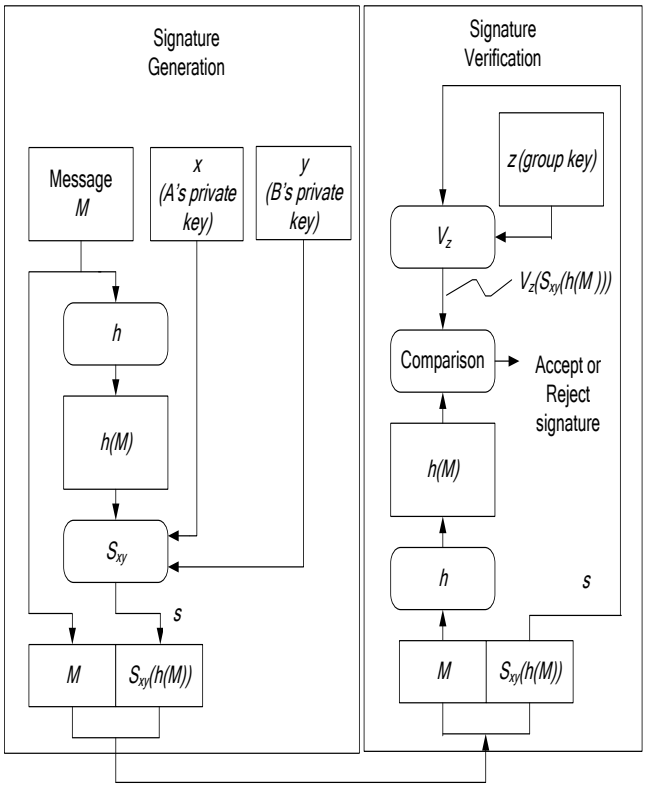



Fig-3: General model for multi-signature scheme

**Key generation:**

RSA multi-signature involves private keys $(x, y)$ for each signer and their group key $z$. The private keys are used for signature generation and a group key for signature verification. The keys for the RSA multi-signature are generated the following way [6] :

(a) Compute $xyz \equiv 1(\mathrm{mod}\,\phi(n))$.

Multi-signature generation:

The first signer should do the following.

(a). Compute $\tilde{m} = h(M)$ an integer in the range $[0; n-1]$.

(b). Compute $s_1 = \tilde{m}^x \bmod n$.

The second signer should do the following.

(a). Compute $s_2 = s_1^{\,y} \bmod n$.

Multi-signature verification:

(a) Compute $\tilde{m}' = s_2^{\,z} \bmod n$.

(b) Verify that $\tilde{m} = \tilde{m}^t$ ; if not, reject the signature.

## 5. LSB Technique

The most widely used technique to hide data is the usage of the LSB [8]. Although there are several disadvantages to this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel.

For example, the following grid can be considered as 2 pixels of a 24-bit color image, using 6 bytes of memory:
(00100111 11101001 11001000)
(00100111 11001000 11101001)

When the character A, whose binary value equals 01000001, is inserted, the following grid results:
(00100**01** 11101**00** 11001**00**)
(00100**01** 11001000 11101000)

## 6. Proposed System

In this section, we describe the proposed adaptive spatial-domain image watermarking technique. The watermark used is a visually meaningful binary image rather than a randomly generated sequence of bits. Thus, human eyes can easily identify the extracted watermark. In fact, embedding a watermark in the least significant bits of a pixel is less sensitive to human eyes. However, the watermark will be destroyed if some common image operations such as low-pass filtering are applied to the watermarked image. Therefore, to make the embedded watermark more resistant to any attack, the watermark must be embedded in the least significant bits by using pseudo-random number generator and permutation table. This will not introduce distortion to the host image and not conflict with the invisible requirement. In addition, to prevent tampering or unauthorized access, the watermark is first encrypted using RSA algorithm into scrambled data. Furthermore, encrypted watermarked image is signed again to acquire authentication and data integrity. The block diagram of proposed watermarking system is illustrated in Fig:

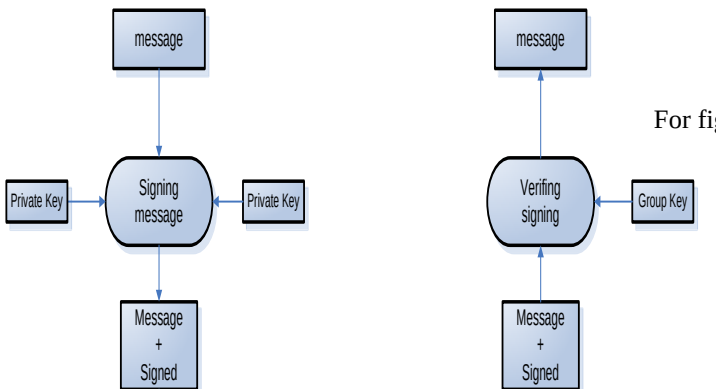



Fig: 4 Block diagram of the proposed system

## 7.Experimental Results

In the experiment, we have calculated and compared the similarity of the following images Fig (a, b, c, d) between original and embedded. We used invisible watermark text for embedding images , tested same watermark text to different images and different watermark text to a single image. The following result we will show is with same watermark text to different images. We have used NC algorithm which is the algorithm when we search similarity of original image and new image which is encrypted/created with text messages added.

We are difficult to distinguish such images since they look almost the same. In this condition, we have to use this NC algorithm ( Normalized cross correlation) to show the robustness/similarity of algorithm under our image. A qualitative estimation of the extracted watermark $\tilde{W}$ ij , with respect to the embedded version $W$ij ,may be expressed as a Normalized Cross Correlation (NC): [7] defined as:

$$NC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{\sum_i \sum_j [W_{ij}]^2}$$

For figure (a)
Original image attribute 67*50= 3350
3350 * 256 = 857,600
Original image size 10.0 KB => 857,600
Embedded image size 9.63 KB ?
= (857,600 * 9.63) / 1
= 825,868.8
= ( 857,600*825,868.8 ) / $(857,600)^2$
= 96.3%

For figure (b)

Original image attribute 60*40 = 2400
2400 * 256 = 614,400
Original image size 7.08 KB => 614,400
Embedded image size 6.60 KB ?
= (614,400 * 6.60) / 7.08
= 572,745.7627
= (614,400*572,745.7627)/ $(614,400)^2$
= 93.22%

For figure (c)
Original image attribute 1024*768 = 786,432
786,432 * 256 = 201,326,592
Original image size 2.25 MB => 201,326,592
Embedded image size 1.15 MB ?
= (201,326,592 * 1.15 ) / 2.25
= 102, 900, 258.1
=(201,326,592*102,900,258.1)/ $(201,326,592)^2$
= 51.1 %

For figure (d)
Original image attribute 1152*864 = 995,328
995,328* 256 = 254,803,968
Original image size 2.84 MB => 254,803,968
Embedded image size 1.10 MB ?
= (254,803,968* 1.10 ) / 2.84
= 98,691,667.75
=(254,803,968*98,691,667.75)/ $(254,803,968)^2$
= 38.8 %

where the maximum value of NCC = 1 corresponds to a perfect match. $W_{ij}$ and $W'_{ij}$ represent the pixel values at locations (i, j) in the original and extracted watermarked images, respectively. The normalized cross correlation value *NC* of the proposed system of Fig:(a) is 96.3%, Fig:(b) is 93.22%, Fig:(c) is 51.1%, Fig:(d) is 38.8%.

Table (1) Similarity of images

| Figure | NC |
|---|---|
| Fig .a | 96.3 % |
| Fig .b | 93.22 % |
| Fig .c | 51.1 % |
| Fig .d | 38.80 % |

Figure(a) is the best because of the following reasons:

(a)Size is reduced not so much from original picture size after text messages is added.

(b)User still can think that the picture is original , since it still looks like original.

(c)The smaller the size from original, the better to transmit.

(d)The normalized cross correlation value NC of figure (a) from all images is 96.3%.

(e)The similarity of original and new images is quantitatively measured by NC and , so Fig (a) is the best we can say.

**Test image**

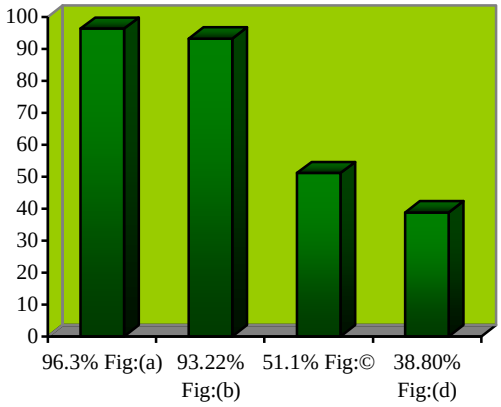

Fig:(a)


Fig:(b)


Fig:(c)


Fig:(d)

**Result (after watermark is inserted)**




**Comparison normalized cross correlation (NC) of 4 pictures**

## 8. Conclusion

This paper proposes a secure verification system for watermarked images with the intention of copyright protection. The proposed system provides the main cryptographic goals: data confidentiality, data integrity and authentication, and non-repudiation. This application will be greatly useful in the governmental departments, such as Immigration, Police and Military (especially in Military Intelligence) where secret communication is vital for national security to transfer copyright protected images as authentication evidence. Moreover, this

application can be used to prevent a buyer from distributing unauthorized image copies and can also be used to prevent a seller from forging the sale transaction of image copies without a buyer.

## Acknowledgements

This paper is being employed under University of Computer Studies (pyay), Ministry of Science and Technology in Myanmar. Last but not least, the author thanks all teachers who gave sound guidelines to complete this work.

## References

[1] Aime` Serge Nguimjeu Ngue`pi, Digital Watermarking, TU- Darmstadt, Deutschland

[2] Image watermarking technique based on the steerable pyramid transform Fadoua DRIRA,Florence DENIS, Atilla BASKURT LIRIS, Laboratoire d'InfoRmatique en Image et Systèmes d'information FRE 2672 CNRS, INSA Lyon, UCB Lyon 1, EC Lyon, Univ. Lyon 2

[3] I Pitas, "A method for signature casting on digital images", Proceedings of IEEE International Conference on Image Processing, Vol. 3, 1996, pp. 215-218

[4] M. M. Yeung and F. Mintzer, "An Invisible Watermarking Technique for Image Verification," IEEE Int. Conf. Image Processing, 1997, vol. 1, pp. 680-683.

[5] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital watermark", Proceedings of IEEE International Conference on Image Processing, Vol. 1, 1994, pp. 86-90.

[6] Satter J. Aboud, Two Efficient Digital Multi-signature Schemes, Department of Computer Science, Faculty of IT, Amman, Jordan

[7] Chiou-Ting Hsu and Ja-Ling Wu, "*Hidden signatures in images*", in Proceedings of International Conference on Image Processing, 1996, pp. 223-226.

[8] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 1998