International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 6, June 2014 ISSN 2319 - 4847

A Novel security techniques based on watermarking and encryption for LSB digital Images

U.V.CHANDRA SEKHAR M.TECH (PH.D) [1], ADARI BHAVANA DEEPTHI [2]
GANDHAM VENKATA HIMAJA [3]

[1]Assistant Professor,CSE Department, Raghu Engineering College
[2, 3]B.tech , Department of Computer Science, Raghu College of Engineering

Abstract

In this paper we proposed a Digital Image Watermarking is the process of embedding information/logo into a digital image which may be used to verify its authenticity or the identity of its owners. If the watermarked image is copied, then the information also is carried in the copy. Many Image watermarking techniques have been proposed. In this paper, we review the various methods, the way they express the watermark and their comparison. This paper investigates the field of image watermarking. This includes a general description of the usage of watermarking and the fundamentals for the different approaches that can be taken when using watermarking. With the development in technology, data transfer of secret information plays a major role. We go for data security in order to prevent the data from hackers and malware infection. In this study, we dealt with the secret key stenography method of hiding a plaintext in an image using a random key.

Keywords: Digital images, watermarking, stego images, image encryption.

1. INTRODUCTION

Pseudo-random number generators are deterministic algorithms that generate a long sequence of digits that statistically resemble a string of truly randomized digits. The digit produced by a pseudo-random number generator is determined by the state of the generator, or the input given to the generator function. The state of the generator changes after a digit is produced. The initial state of a generator is based on a seed value supplied by the user, and this state is referred to the seed state. The set of all possible seed values is called the seed domain. This is where the “pseudo-random" part of the name comes from; given a specific state, a pseudo-random number generator will always produce the same digit. In this sense, a pseudorandom number generator is never truly random. It is important to note that all pseudo-random number generators are periodic. Eventually, the sequence will repeat itself. If the state of the generator contains n bits, then the period of the pseudo-random sequence has a maximal period of 2n bits. There are ways to generate truly random sequences of numbers, but they are all hardware based. Some examples include measuring the elapsed time between emissions of particles in 24 radioactive decay or thermal noise from a resistor. However, it is impractical to use these methods for modern applications that require a random string of digits. Many different algorithms exist for computing pseudo-random sequences and they typically leverage a computationally difficult problem, such as the factorization of large integers or the discrete logarithm problem, to ensure the security of the generator’s state. This makes pseudo-random number generators well-suited for cryptography since the secret state can act as a shared key between two parties.
A pseudo-random number generator is considered cryptographically secure if it satisfies the following properties:
1. Given k digits of a pseudo-random sequence, there is no polynomial-time algorithm that can predict the (k + 1)th digit of the sequence, and
2. Should the state of the generator become compromised, there is no polynomial-time algorithm that can reproduce the string of pseudo-random digits prior to the state. In other words, the previous states of the generator cannot be determined from the known state.

Image watermarking became popular in the 1990s because of the widespread of the Internet. A hidden watermark message is inserted into a host image such that the hidden message will survive intended or unintended attacks. The first example of a technology similar to digital watermarking is a patent filed in 1954 by Emil Hembrooke for identifying music works. In 1988, Komatsu and Tominaga appear to be the first to use the term “digital watermarking” [1]. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. The information/logo are embedded in image is called a digital image watermark. The information/logo where the watermark is to be embedded is called the host image [2, 3].

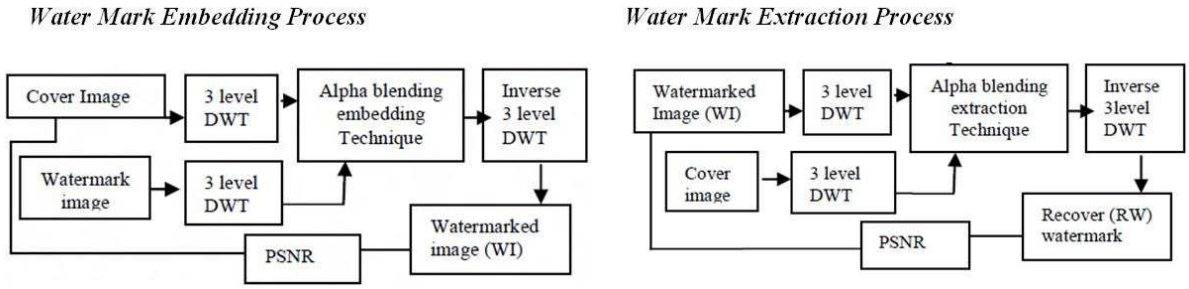
Digital image watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital image watermarking a secret information/logo is imperceptibly embedded in another image. The secret information/logo is called watermark and it depicts some metadata, like security

or rights information about the main image. The main image in which the watermark is embedded is referred to as cover image since it covers the watermark. The digital image watermarking system essentially consists of a watermark embedded and a watermark detector as shown in figure 1.1.

Figure 1.1 Digital Image Watermarking

The watermark embedder inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo. Sometime a watermark key is also used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark information/. The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital image watermarking techniques should be resilient to both noise and security attacks [7].

1. 1 TYPES OF WATERMARKING



Various types of watermarking techniques having different applications are given below.

1) Inserted Media Category:
Watermarking techniques can be categorized on the basis of whether they are used for Text, Image, Audio or Video.
2) Robust & Fragile Watermarking:
In robust watermarking, the modification to the watermarked content will not affect the watermark whereas fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered.
3) Visible & Transparent Watermarking:
Visible watermarks are ones, which are embedded in visual content in such a way that they are visible when the content is viewed. Transparent watermarks are imperceptible and they cannot be detected by just viewing the digital content.
4) Public & Private Watermarking:
In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not authorized to detect the watermark.
5) Asymmetric & Symmetric Watermarking:
Asymmetric is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking the same keys are used for embedding and detecting watermarks.

1.2 CLASSIFICATION OF DIGITAL IMAGE WATERMARKING TECHNIQUES

There are various technique used to hidden message/logo in images and are classified as

A. Least Significant Bit Modification

The simpler method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object [9]. LSB substitution however has lots of drawbacks. Any addition of noise or lossy compression is likely to defeat the watermark. If we simply set the LSB bits of each pixel to one the watermark obsolete with negligible impact on the cover object. An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key [9]. Security of the watermark would be improved as

the watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant.
Pixel Value of Image: 11001010 00110101 00011010… Watermark: 1 1 1…
Watermarked Image: 11001011 00110101 00011011…

B. Correlation-Based Techniques

Another technique for watermark embedding is to exploit the correlation properties of additive pseudorandom noise patterns as applied to an image. A pseudorandom noise (PN) pattern W(x,y) is added to the cover image I(x,y), given in the equation 1.1.

$$I_w(x, y) = I(x, y) + k * W(x, y) \quad \text{..... 1.1}$$

k denotes a gain factor, and I_w the resulting watermarked image. Increasing *k* increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block. This basic algorithm can be improved in a number of ways. First, the notion of a threshold being used for determining a logical "1" or "0" can be eliminated by using two separate pseudo-random noise patterns. One pattern is designated a logical "1" and the other a "0". The above procedure is then performed once for each pattern, and the pattern with the higher resulting correlation is used. This increases the probability of a correct detection, even after the image has been subject to attack. We can further improve the method by pre-filtering the image before applying the watermark. If we can reduce the correlation between the cover image and the PN sequence, we can increase the immunity of the watermark to additional noise. By applying the edge enhancement filter given in equation 1.2, the robustness of the watermark can be improved with no loss of capacity and very little reduction of image quality.

$$F_{edge} = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix}$$

C. Wavelet Watermarking Techniques

Another possible domain for watermark embedding is that of the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), Vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" Wavelet decomposition, as in the 2 scale wavelet transform shown below in figure 1.3. One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. One of the most straightforward techniques is to use a similar embedding technique to that used in the DCT, the embedding of a CDMA sequence in the detail bands according to the equation 1.5.

$$I_{W_{u,v}} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases}$$

Where Wi denotes the coefficient of the transformed image, xi the bit of the watermark to be embedded, and α a Scaling factor. To detect the watermark we generate the same pseudo-random sequence used in CDMA generation And determine its correlation with the two transformed detail bands. If the correlation exceeds some threshold T, The watermark is detected.

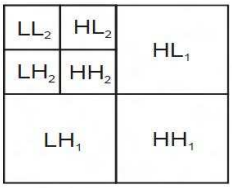


Figure 1.2: 2 Scale 2-Dimensional Discrete Wavelet Transform

This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for each PN sequence, which is then added to the detail coefficients as per equation 1.5. During detection, if the correlation exceeds T for a particular sequence a "1" is recovered; otherwise a zero. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered. Furthermore, as the embedding uses the values of the transformed value in embedded, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients. The author [11] claims that the technique should prove resistant to JPEG compression, cropping, and other typical attacks.

2. RELATED WORK

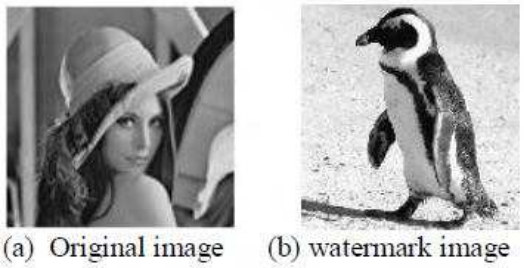


Figure 1.3 : LSB Method (a) Original Image (b) Logo (c) Watermarked Image (d) Extracted Watermark

Table 1: Various Quality Measures of image using LSB Method

Image	PSNR	MSE	Average Difference	Maximum Difference
Lena	58.3101	0.0960	-0.1487	0
Pepper	58.3101	0.0960	-0.1267	0
Cameraman	58.3101	0.0960	-0.1487	0
DAVIET	58.3101	0.0960	-0.1363	0

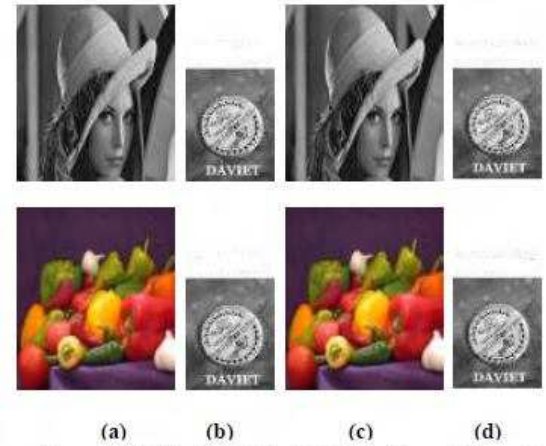


Figure 1.5 :Modified LSB Method (a) Original Image (b) Logo (c) Watermarked Image (d) Extracted Watermark

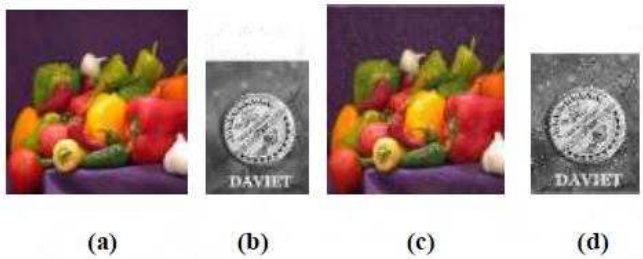


Figure 1.4: LSB Method (a) Original Image (b) Logo (c) Noisy Watermarked Image (d) Extracted Watermark

Table 2: Various Quality Measures of noisy images using LSB Method

Image	PSNR	MSE	Average Difference	Maximum Difference
Lena	18.0868	1.0102 x 103	-1.6128	191
Pepper	17.7297	1.0968 x 103	-2.2045	226
Cameraman	18.0092	1.0284 x 103	-0.7614	170
DAVIET	18.2350	976.3006	1.2388	244

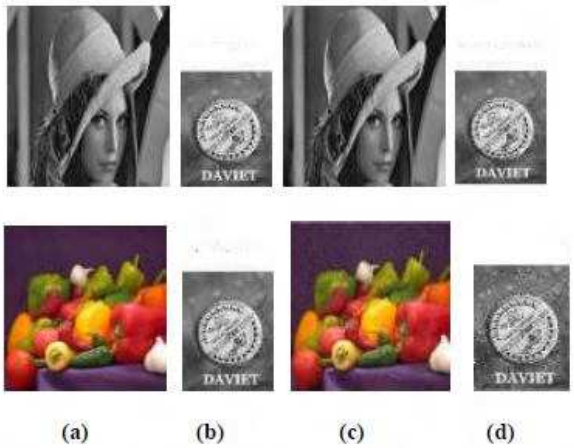


Figure 1.6: Modified LSB Method (a) Original Image (b) Logo (c) Noisy Watermarked Image (d) Extracted Watermark

Table 3: Various Quality measures of image using Modified LSB Method

Image	PSNR	MSE	Average Difference	Maximum Difference
Lena	66.7597	0.0137	-0.1484	0
Pepper	66.7597	0.0137	-0.1268	0
Cameraman	66.7597	0.0137	-0.1484	0
DAVIET	66.7597	0.0137	-0.1367	0

Table 4: Various Quality measures of noisy images using Modified LSB Method

Image	PSNR	MSE	Average Difference	Maximum Difference
Lena	26.5925	142.5050	-1.6262	181
Pepper	26.1334	158.3931	-2.2457	199
Cameraman	26.4360	147.7343	-0.6749	203
DAVIET	26.7448	137.5949	1.1256	245

3. CONCLUSION

We survey and review number of techniques for the watermarking of digital images, as well as compares their limitations and possibilities. We proposed a modified LSB method and give the brief description of digital image watermarking. LSB substitution is the simplest technique but not a very good candidate for digital watermarking due to its lack of robustness. LSB embedded watermarks can easily be removed or altered without degrade the image quality however the modified LSB method improves the results. Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique and Pseudo-Random Encoding Technique on images to obtain secure stego-image. Table 2 and Table 3 shows that PSNR of Pseudo random encoding is higher than PSNR of LSB encoding. Our results indicate that the LSB insertion using random key is better than simple LSB insertion in case of lossless compression. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both grayscale and color image. This paper focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

REFERENCES

[1] Frank Hartung, Martin Kutter, "Multimedia Watermarking echniques", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103, July 1999.

[2] "Digital Watermarking" available at http://en.wikipedia.org/wiki/Digital_watermarking

[3] Alper Koz, "Digital Watermarking Based on Human Visual System", The Graduate School of Natural and Applied Sciences, The Middle East Technical University, pp 2 – 8, Sep 2002.

[4] J.J.K.O. Ruanaidh, W.J.Dowling, F.M. Boland, "Watermarking Digital Images for Copyright Protection", in IEE ProcVis. Image Signal Process, Vol. 143, No. 4, pp 250 - 254. August 1996.

[5] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" submitted at University Salzburg, pp. 9 – 17, Jan 2000.

[6] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, "A SURVEY ON WATERMARKING APPLICATION SCENARIOS AND RELATED ATTACKS", IEEE international Conference on Image Processing, Vol. 3, pp. 991 – 993, Oct. 2001.

[7] Saraju Prasad Mohanty, "Watermarking of Digital Images", Submitted at Indian Institute of Science Bangalore, pp. 1.3 – 1.6, January 1999.

[8] N.F. Johnson, S.C. Katezenbeisser, "A Survey of Steganographic Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75

[9] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000.

[10] J.R. Hernandez, M.Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure", in IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000.

[11] H. Inoue, A. Miyazaki, T. Katsura "An Image Watermarking Method Based on the Wavelet Transform", Kyushu Multimedia System Research Laboratory.

AUTHORS

U.V.CHANDRA SEKHAR, M.TECH (PH.D), Assistant Professor, CSE Department, Raghu Engineering College, Visakhapatnam, Andhra Pradesh.

ADARI BHAVANA DEEPTHI, B.tech CSE Department, Raghu Engineering College, Visakhapatnam, Andhra Pradesh..

GANDHAM VENKATA HIMAJA, B.tech CSE Department, Raghu Engineering College, Visakhapatnam, Andhra Pradesh.. .