Embedding Algorithm using multiple pseudo random number generators with LSB technique

خوارزمية تضمين العلامة المائية بإستخدام مولد الارقام العشوائية
المتعدد مع تقنية البت الاقل اهمية

Professor Dr. Hamza A. A. Al_Sewadi
Aysar Sh. Alsaadi

Middle East University
Computer Science Dept, Amman, Jordan

Abstract:

Digital Watermarking is a technique for embedding personal or confidential information within an image; video or text .The paper proposes an embedding method that implements multiple pseudo random number generators the cover image file will be segmented into number of block each contains a specific pixels length. The first PRNG is used to generate secret key by chaotic map for encrypting the logo image before the embedding process, the second PRNG generates random number that to be used for randomly selecting the pixels from each block to be modified with watermark bits by LSB method. The randomness of the keys has a strong impact on the system's security strength for being difficult to be predicted, guessed, reproduced, or discovered by a cryptanalyst. Obtained results were satisfactory and suggest that, this technique would be suitable for applications involve cryptography, steganography, and copyright protection.

Keywords: PRNG, Copyright, Cryptography, Steganography, Digital watermarking.

المستخلص:

العلامة المائية وهي تقنية تستخدم لتضمين المعلومات الشخصية او السرية داخل صورة او فيديو او داخل نص كتابي. طريقة الخوارزمية المقترحة هي تقسيم الصورة الاصلية التي سيتم اخفاء المعلومات داخلها الى عدة اجزاء بحيث كل جزء من الصورة يحتوي على طول معين من البكسل. تشتمل الخوارزمية المقترحة على مولدين للارقام العشوائية حيث يستخدم مولد الارقام العشوائية الاول لتوليد مفتايح سرية بواسطة خارطة عشوائية وذلك لتشفير هذه المعلومات قبل عملية اخفاءها داخل الصورة. بينما يستخدم مولد الاقام العشوائية الثاني سلسلة من الارقام العشوائية تستخدم لتحديد موقع البايت داخل كل جزء من الصورة الاصلية ليتم التعديل على بتات صورة الشعار، اما المعلومات فيتم اخفاءها بواسطة تقنية البت الاقل اهمية (LSB). المفتاح العشوائي له تاثير قوي جدا على قوة امنية بيانات الأنظمة، وليس من السهل على اي محلل شفرات اكتشافه او التنبؤ به. وبينت النتائج التجريبية لهذه الخوارزمية في هذا البحث بانها تقنية مناسبة للتطبيقات الامنية (علم التشفير،علم الاخفاء وكذلك حماية حقوق النشر) و من خلال اخفاء معومات مهمة او تواقيع تخص المالك الفعلي للوسائط المتعددة.

الكلمات المفتاحية:مولد الارقام العشوائية، حقوق النشر، علم التشفير، علم الاخفاء، العلامه المائية.

1. Introduction:

Today's generation witnesses the developments of digital media. The simplest example of digital media is a photo captured by phone camera. The use of Digital media is common in present era. Other example of digital media is text, audio, video etc. [1], the process of digital watermarking (DW) involves tweaking pixel value at various regions with them an image to encode some piece of information. This encoded information can be used to provide copyright information, to prevent illegal duplication, or even as a dynamic link between the image and online digital data. For most applications, the image owner would like to make the encoded data robust enough to ensure its detection while maintaining the high quality the original image. [2]

DW can be visible or invisible [3]. In the case of visible watermarking, watermarks are embedded in such a way that they are visible when the content is viewed. Invisible watermarks cannot be seen with the naked eye but they can be recovered using an appropriate decoding algorithm [4]. Based on the type of document to be watermarked, watermarking can be classified as image watermarking, video watermarking and audio watermarking [5].

DW techniques can be achieved in two domains either spatial domain or transform domain. Spatial domain works directly on the pixel, by modifying the carrier image pixel value for embedding the watermark data. The Least significant bit (LSB) is most commonly used with spatial domain. Transform domain is embedding the watermark by modifying the transform domain coefficients using one of the transformation techniques, such as discrete cosine transform (DCT), discrete wavelet transforms (DWT) and discrete fourier transform (DFT) [6]. Table 1 which show the differences between theses watermarking techniques by summarizing their advantage and disadvantages. [7] [8].

2. The proposed algorithm:

The proposed watermarking scheme consist a number of steps in order to give a proper, secure, and high authenticated model that serve the ownership or the personal data to be transferred through the internet. The main stapes in illustrate in the figure (1), (2) to shown a simple embedding and extracting method, which will clarify the process in section 2.1

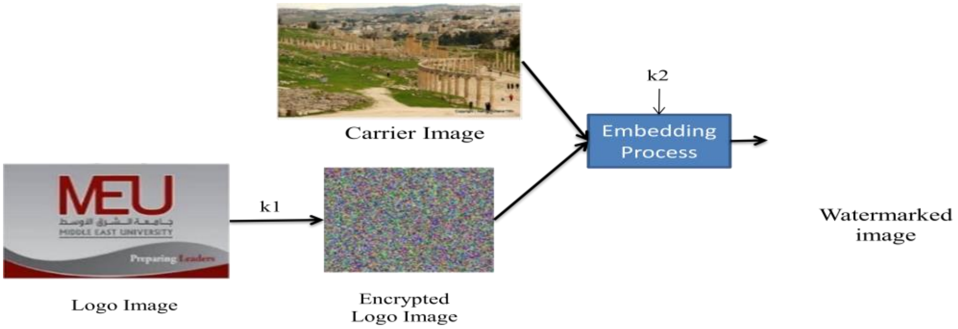

Figure (1) Embedding Process

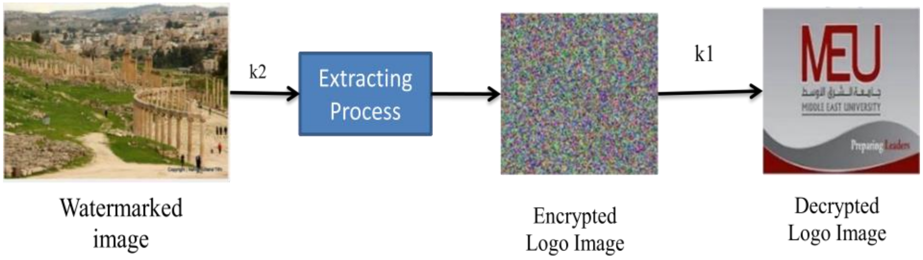

Figure (2) Extracting Process

2.1 Watermark embedding process

The main objective of the proposed embedding algorithm is to increase the watermark robustness in order to get high authentication copyright protection against many attacks that aim to copy, manipulate or damage the personal data. The algorithm relies on the randomness concept by implementing multiple pseudo random number generator (PRNG) for embed a logo image into the carrier image. To PRNG's are implemented, the first PRNG is a modified Lorenz attractor. It is involved to encrypt the logo image before embedding process. The other PRNG is implemented for embedding the encrypted logo into the carrier image with LSB technique; the proposed algorithm consists of three processes; preparation, embedding and extraction as follow:

a. Preparation process

In this process, random numbers are generated to be used for embedding locations, logo image, carrier image are selected, and then some calculations are done to determine the parameters in the following steps.

Step1: PRNG's preparations

Two PRNG's are selected to be used for both encrypting the logo image and locating embedding places in the carrier multimedia. The chosen PRNG's were Lorenzo and trivium. They were chosen for their sound randomness, besides they were also modified by another's to suit the intended purpose. One seed key (k_1) is selected as secret key for encryption another seed key (k_2) for embedding. The modified PRNG's will be explained later.

Step 2: Select a logo image (W) and calculate its length (L_w) in bits.

Step 3: Select a carrier image (C), calculate its length(L_c) in bits.

Step 4: Segment the carrier image into a number of blocks (B), each of length N-bits according to equations (1) and (2).

$$\boldsymbol{B = \frac{(L_c)}{8*L_w}} \text{ ……………………………………………… } \mathbf{(1)}$$

$$\boldsymbol{N = \frac{(L_c)}{K}} \text{ ……………………………………………… } \mathbf{(2)}$$

b. Embedding process:

For the embedding of the logo image into the carrier image, the block diagram of Fig (3) is followed. It consists of the following steps.

Step1: use seed key K_1 to generate a sequence of random numbers by the modified Lorenzo PRNG.

Step 2: Encrypt the logo W using the random numbers generated in step1, to get (W_e) by the equation (3)

$$\boldsymbol{W_e = E_{K1}\ (W)} \text{………………………………………} \mathbf{(3)}$$

Step 3: use seed key (k_2) to generate a sequence of random numbers by modified trivium PRNG.

Step 4: embed the resulting encrypted watermark (W_e) into the carrier image C using the random number sequence generated in step 3, by equation (4)

$\boldsymbol{C_{we} = E_{k2}\ (W_e)}$**.. (4)**

Now C_{we} is the watermarked image which can be publicly used with its copyright protection measure. Figure (1) shows the steps of embedding process.

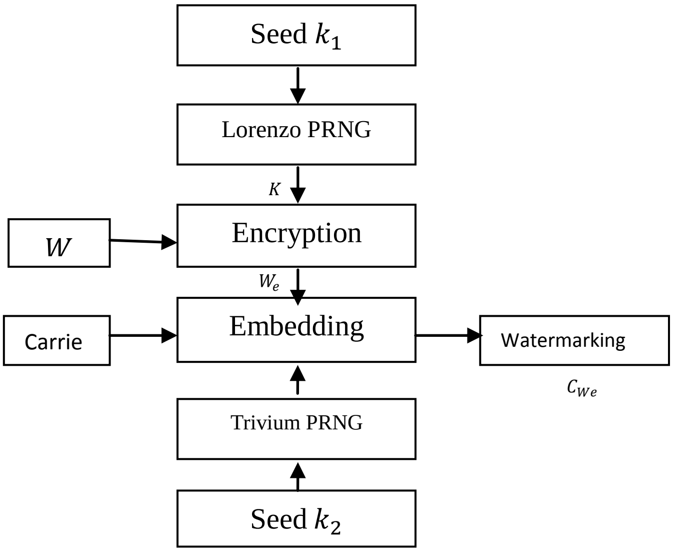

Figure (3) embedding process

c. Extraction process:

To extract the embedded logo image from the watermarked image, a process similar to embedding process is conducted but in reverse order. It starts with watermarked image (C_{we}), using the same keys sequence generated by Trivium PRNG first to get W_e , then using the same keys sequence generated by Lorenzo PRNG to decrypt W_e in order to produce W, figure (4) is illustrate extraction process.

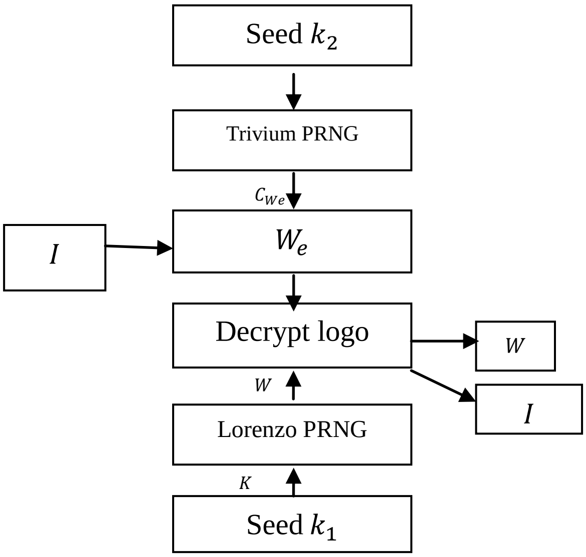

Figure (4) Extraction process

2.2 Modified Lorenz attractor PRNG:

The first step in this model process is the encryption of the logo bits stream using modified Lorenz chaotic equation which is a 3D dynamical system defined by x, y and z. Lorenz equation is a model of thermally induced fluid convection in the atmosphere. It is among the classical chaotic systems and implies as the cause of the “butterfly effect” in the scientific studies due to the fact that the attractor has two wings as the butterflies. Therefore, it has been widely studied in chaos theory, dynamic system modeling, chaotic control and synchronization phenomenon. The equation system gives a chaotic behavior with regard to the initial system parameters. Apart from any 1D or 2D chaotic systems, the Lorenz system has a much complicated chaotic behavior. The equation system contains three differential equations:

$$x_{i+1} = a(y_i - x_i) \text{..} (5)$$

$$y_{i+1} = rx_i - y_i - x_i z_i \text{..................................} (6)$$

$$z_{i+1} = x_i y_i - bz_i \text{..} (7)$$

Here x, y and z are the functions of time with the derivative forms (i.e. *x*, *y* and *z*) and *a*, *b*, *r* are the system parameters for the deterministic system.

All numbers in this technique represent real numbers with randomness property.

Some of modifications are proposed to be more suitable in the random watermarking technique by the following equations, where the chaotic random number sequence denoted by the

Seq_j:

$$Seq_j = \lfloor x_{i+1} * 1000 \rfloor \bmod 256 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(8)$$
$$Seq_{j+1} = \lfloor y_{i+1} * 1000 \rfloor \bmod 256 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(9)$$
$$Seq_{j+2} = \lfloor z_{i+1} * 1000 \rfloor \bmod 256 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(10)$$

In this operation the first three digit after floating point part are moved to integer side with truncate then the mod 256 operation convert these three digit number into byte form to be XORed with input image.

Equation (5) presents the main steps of the secret image encryption operations with the following initial values of Lorenzo Attarctor are:

A = 10 , b = 28 , r =2.66666666676.

Also the standard parameters of lorenzo are public but the input values of X, Y and Z are secret values, these values are converted into integer values according the above equations to generate secret chaotic sequence according the following equation:

$$x_{i+1}{}' = x_{i+1} * 10000000 - \lfloor x_{i+1} * 10000000 \rfloor \ldots\ldots\ldots\ldots(11)$$
$$y_{i+1}{}' = y_{i+1} * 10000000 - \lfloor y_{i+1} * 10000000 \rfloor \ldots\ldots\ldots(12)$$
$$z_{i+1}{}' = z_{i+1} * 10000000 - \lfloor z_{i+1} * 10000000 \rfloor \ldots\ldots\ldots\ldots(13)$$

3. The modified Trivium PRNG:

The second PRNG is a modified version of Trivium pseudo-random number generator. It is accomplished by using Linear Feedback Shift Registers (LFSR) based Pseudo Random Generator (PRNG). The modifications will include: bit lengths, XOR selected sections and some other bits for initialization. This proposed PRNG will be initialized by two vectors; first, the secret key of length 12 characters (chosen here as Hello Jordan), which will be converted into 84 bits using ASCII codes, and second, the initial vector s_j which is 87 bits, also. It is fixed for each user in the algorithm. This PRNG will be involving in the embedding of encrypted logo process randomly in the carrier image.

$t_i = s_{j+1} \oplus s_{j+2}$ .... (14)

$z_i = t_{j+1} + t_{j+2} + t_{j+3}$ .... (15)

Where $t_i$summation for each shift register is z_i is key generation for each t_i, the generated number from the equations (14) and (15) represent the byte location in each block within the carrier image.

4. Algorithm Performance and Results

The performance evaluation of the proposed watermarking scheme is obtained by measuring imperceptibility, robustness and encryption of the resulting watermarked images by using a various image (Carriers) and logo sizes. The error metrics used to test the proposed algorithm are Peak Signal to Noise Ratio (PSNR), Correlation (RC) and mean square error (MSE), number pixel change ratio (NPCR). The algorithm implemented on logo dimensional 160*149 and cover high resolution with dimensional 3818*2540, the number of blocks are 485.The test results of the encryption of logo image and embedding tests showing in the table (1).

Table (1) Encryption and embedding result

Encryption		Embedding	
E-PSNR	10.2034405 db	PSNR	77.942263 db
E-MSE	12699.7082	MSE	0.00102012
H-CR	0.96615125	H-CR	0.99958
V-CR	0.98825802	V-CR	0.99940
D-CR	0.91973564	D-CR	0.99949
E-NPCR	100%	NPCR	0.31083594

5. Conclusion:

A new efficient and accurate algorithm has been developed and investigated for digital watermarking for both color and grayscale images with deferent sizes. The proposed method produces watermarks that are imperceptible by visual inspection watermarking. The used technique is based on the spatial domain using LSB method together with incorporation of two modified PRNG's for encrypting the logo images and selecting random pixels in the carrier image. Encrypting the logo image by one PRNG as first step, and then embedding the encrypted logo bits into the carrier image randomly using second PRNG makes the hacking task very hard and complex to guess the watermarked image or secret keys that used in encryption and embedding technique. Hiding is finally given. The obtained results of PSNR, MSE, CR and NPCR show the effectiveness of the proposed Watermark image technique.

Reference

[1] Saini, L. K., & Shrivastava, V. (2014), “a survey of digital watermarking techniques and its applications”, *ArXiv preprint arXiv: 1407.4735*.
[2] Hannigan, B. T., Reed, A. M., and Bradley, B. A. (2001, August),” Digital watermarking using improved human visual system model”, In *Photonics West 2001-Electronic Imaging* (pp. 468-474). International society for optics and photonics, pp468-474).
[3] Z. Jalil, A. M. Mirza (2009), “A Review of Digital Watermarking techniques for text documents”, IEEE,
[4] Jaseena, K. U., & John, A. (2011), “Text watermarking using combined image and text for authentication and protection”, International journal of computer applications, *20*(4), 8-13.

[5] M. Chandra, S. Pandey, R. Chaudhary (2010), “Digital watermarking techniques for Protecting digital Images”, IEEE.
[6] Jiang Xuehua, “Digital Watermarking and Its Application in Image Copyright Protection‖”, 2010 International Conference on Intelligent Computation Technology and Automation.
[7] Amit K. S., Nomit S., Mayank D., Anand M. (2012), “A Novel Technique for Digital Image Watermarking in Spatial Domain‖”, 2nd IEEE international conference on parallel, Distributed and grid computing.
[8] Scholar, P. G. (2014), “A survey: digital image watermarking techniques. Int. J. Signal Process. Image Process”. Pattern Recognit, 7(6), 111-124.