[Volume 4 issue 05 May 2016]
PageNo.1325-1332 ISSN : 2320-7167

INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH

On Watermarking Using Arnold and Wavelet Transform

Dr. Narendra kumar Ramchandra Dasre, Ph. D.

Associate Professor, Department of Engineering Sciences, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India, narendasre@rediffmail.com

Corresponding Author:

Dr. Narendrakumar Ramchandra Dasre

Associate Professor,

Department of Engineering Sciences, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai,

Maharashtra, INDIA Pin-400706

Email: narendasre@rediffmail.com

ABSTRACT

This paper presents a robust but secured blind digital image watermarking algorithm based on two dimensional discrete wavelet transform. The algorithm is robust because instead of inserting watermark image as it is in a wavelet channel, the watermark image is compound encrypted using Arnold transform and Logistic mapping and then inserted into the desired wavelet channel. The algorithm proposed is secured because there are many parameters that can be used as a security key e.g. the initial value of the Logistic mapping parameters and the iterative time of the Arnold transform. It is also possible to change the initially selected parameters. The algorithm was tested using different powerful attacks like bit compression, JPEG compression, median filtering, image cropping etc. The Experimental result found supports the robustness and security of the proposed algorithm.

Keywords: Compound encryption, Arnold transforms, Logistic mapping, Normalized correlation coefficient, PSNR.

TITLE: On Watermarking Using Arnold and Wavelet Transform.

1 INTRODUCTION

Due to the rapid growth of communication technology, the whole world has come closer. Growth in communication technology gave birth to the Internet. The Internet allows distribution of multimedia information in an effortless and timeless manner. A free download environment and a more powerful image processing softwares present great challenges to copyright protection and authentication of multimedia data. To protect digital data from unauthorized copying and illegal distribution, digital watermarking provides the best potential solution. Hence off late, it has attracted researcher and software creators and has encouraged them to develop more powerful digital watermarking algorithms that will satisfy all the requirements of watermarking system [1].

Watermarking is a process of embedding information or code into image, audio or video objects which may be visible or invisible. Classification of watermarking in all possible ways is given in figure 1.

Watermarking techniques mainly falls in two categories-spatial domain method [2, 3] and spectral domain method [4, 5].

a) Spatial domain method: In this, watermark is embedded directly by modifying the pixel location of the images. These methods are less complex as no transform is used but are not robust against attacks. For example, simple image cropping operation may eliminate the watermark. They also have relative low bit embedding capacity and are not enough resistant to lossy image compression. The simplest example based on these methods is to embed the watermark in the Least Significant Bits (LSB) of image pixels [6].

b) Spectral domain method: In these methods, the image is transformed into a set of a frequency domain coefficient using discrete cosine transform(DCT), discrete Fourier transform(DFT) or the discrete wavelet transform(DWT). Watermark is inserted into an image by modifying selected frequency coefficients of image pixels. These methods can embed more bits of watermark and are more robust to attacks.

But both of the techniques discussed above have the same defect that is they modify the working pixels of original image.

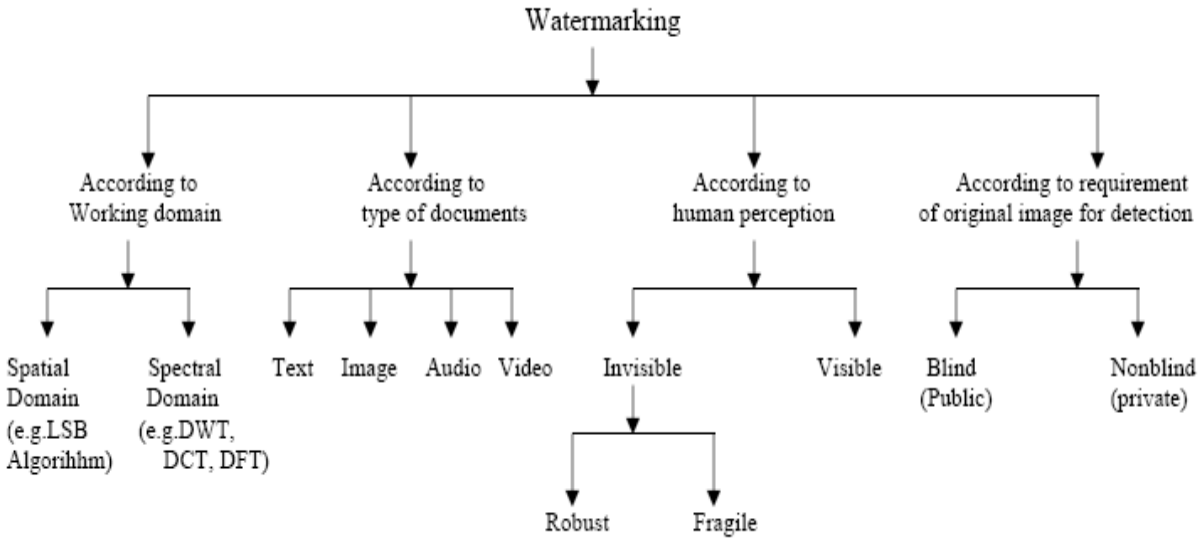

Figure 1. Classification of Watermarking

2 PRELIMINARY NOTES

a) Discrete wavelet transform of the image:

The wavelet transform is identical to a hierarchical sub-band system where the sub-bands are logarithmically spaced in frequency. The basic idea of the DWT for a two dimensional image is described as follows. An image is first decomposed into four parts of high, middle and low frequencies (i.e. LL1, HL1, LH1, HH1 sub-bands) by critically sub-sampling horizontal and vertical channels using Daubechies filters as given in [7]. The sub-band HL1, LH1 and HH1 represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficient, the sub-band LL1 is further decomposed and critically sub-sampled. This process is repeated several times which is determined by the application in hand. An example of an image

decomposed into ten sub-bands for three levels is shown in Figure 2. Each level has various bands information such as low-low, low-high, high-low and high-high frequency bands.

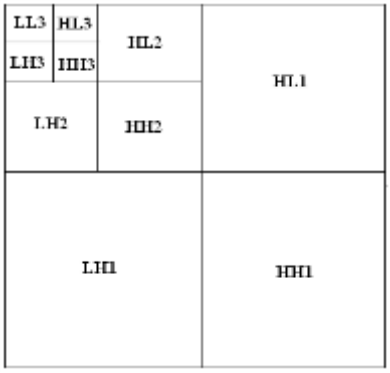

Figure 2. Three level wavelet decomposition

Furthermore, from these DWT coefficients, the original image can be reconstructed. For the reconstruction process, the same filter must be used. This reconstruction process is called the inverse DWT (IDWT). If I(m, n) represent an image, the DWT and IDWT for I(m, n) can be similarly defined by implementing the DWT and IDWT on each dimension m and n separately.

b) Logistic mapping techniques:

To generate a perfect random sequence, we will use the chaotic map. Because it has been found that chaotic signals are a kind of pseudo-random irreversible and dynamic signal generated by deterministic nonlinear equations which possesses good characteristics of pseudorandom sequences. The Chaotic Theory has significant applications in digital communication such as spectrum communication systems, crypto systems and signal processing [8]. Here, consider a distinguishing Chaotic map called Logistic which is defined as –

$$X_{n+1} = \mu X_n (1 - X_n) \qquad \text{Where } 0 \leq \mu \leq 4 \text{ and } X_n \in [0, 1]$$

With $3.569945 \leq \mu \leq 4$, chaotic system is highly sensitive to initial parameters. The system can be made to run in different orbits by selecting different initial parameters. The output sequence generated has good randomness, correlation, complexity [9] and is similar to white noise.

Having Generated the sequence, we will then convert into the sequence of 0s and 1s by applying the threshold. To set the threshold, we will take the mean of the generated sequence. If the element of the generated sequence is greater than the threshold then replace that element by one, otherwise by zero.

c) Arnold transform:-

Arnold transform is used to scramble the digital image. The digital image is nothing but matrix of pixels. Each pixel has a unique position in terms of image height and width and has different gray level value. For a digital image with size N×N, cat mapping of pixel co-ordinate (x, y) is

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

Where x, y ε {0, 1, 2……N-1}. Here, mod N represents the modulo operation and (x′ y′) represents new position of pixel after scrambling by Arnold transform. In order to guarantee that cat mapping is one to one mapping , the value of the matrix A should meet the requirement of |A| =1. So the matrix A can be simply given by

$$A = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix}$$

where a and b both are integers. The basic function of cat mapping is to arrange the location of pixels within the image. It achieves its objectives of encryption by disturbing the position of pixels [10, 11]. The iterative formula of cat mapping can be expressed as- $P_{x,y}^{n+1} = AP_{x,y}^{n}$ mod N,

$P_{x,y}^{n}$ =(x, y)^{T} and n = 0, 1, 2, …. where n is the times iterative transformation and A is matrix of Arnold transform. Because of the limit of N×N pixel performance, the process has iteration period. The period of the iteration [12] is given as in table1.

TABLE 1: THE RELATION BETWEEN IMAGE SIZE AND THE ITERATION PERIOD OF ARNOLD TRANSFORM

N	2	4	5	8	10	16	32	64	128	256
period	3	3	10	16	30	12	24	48	96	192

Once cat mapping is applied to the original watermark image W_0, it is easy to get W_0 back by taking inverse Arnold transform until iteration period.

3 ALGORITHM:

In this section, we consider the algorithms for the embedding and extracting of watermark.

A) WATERMARK EMBEDDING:

Here, we consider the steps in algorithm for embedding the watermark in the host image.

1) Let I_0 be a original image of size $N_1 \times N_2$ and W_0 be a original binary watermark image of size $M_1 \times M_2$.Generate a PN sequence by logistic mapping of length $M_1 \times M_2$. Resize it into a matrix Of $M_1 \times M_2$.
2) Apply Arnold transform to original watermark W_0 of size $M_1 \times M_2$ to get encrypted watermark W_r.
3) Take XOR between resized matrix of PN sequence and encrypted watermark W_r to get compound encrypted watermark W.
4) Perform the three level decomposition of image I_o using two dimensional discrete wavelet transforms.
5) Embed the compound encrypted watermark W in a wavelet channel C of image I_0 according to

[13] by following equation,

$$C(n,m) = \begin{cases} C(n,m) & \text{if } 0 \le n < \frac{N_1}{8} - M_1 \text{ and } 0 \le m < \frac{N_2}{8} - M_2 \\ k.M(n - \frac{N_1}{8} + M_1, m - \frac{N_2}{8} + M_2) & \text{otherwise} \end{cases}$$

where $0 \le n \le N_1/8$ and $0 \le m \le N_2/8$.

6) Take inverse discrete wavelet transform of image obtained in step (5) to get watermarked image I_W. Note that $I_0 = I_W$, theoretically.

B) WATERMARK EXTRACTION:

In this subsection, we consider the steps to extract the watermark from the watermarked image.

1) Perform the three level decomposition of the watermarked image I_W using DWT.
2) Extract the compound encrypted watermark W' from watermarked image I_W by following equation. Note that $W = W'$ theoretically.

$$W'(n.m) = k^{-1} C(n + \frac{N_1}{8} - M_1, m + \frac{N_2}{8} - M_2)$$

Where $0 \le n \le M_1$ and $0 \le m \le M_2$. Scaling factor k lies between 0 and 1.

4 THE EXPERIMENTAL RESULTS

We tested the proposed algorithm on 256 ×256 Lena gray level image. The original binary watermark W_0 of the size 32×32 was scrambled with 24 times Arnold transform iteration and with logistic mapping parameter μ=3.8, x_0=0.5 and threshold T, compound encrypted watermark W was formed and inserted into wavelet channel. The values μ, x_0, T can be used as a security key. All these parameters can be changed from time to time to provide flexibility.

Figure 3 shows original image I_0, watermarked image I_W, inserted watermark W and extracted watermark W'. Figure 4 shows watermarked image I_W and extracted watermark W' after median filtering attack. Figure 5 shows watermarked image I_W and extracted watermark W' after image cropping attack. Figure 6 shows watermarked image I_W and extracted watermark W' after JPEG compression. Figure 7 shows watermarked image I_W and extracted watermark W' after bit compression.

a) Invisibility testing of watermarked image:
The inserted watermark into an image I should not provide any visible artifacts noticeable to human eye i.e. I_0 and I_W must be exactly the same. The extent up to which this is achieved, is expressed by Peak Signal to Noise Ratio (PSNR). PSNR of image of size N×N is given by following equation:

$$PSNR = 10 \log_{10} \left[\frac{N \times N \times \max(I_w)^2}{\sum_{i=1}^{N} \sum_{j=1}^{N} (I_0 - I_w)^2} \right]$$

Where $I_0(i, j) = I_0$ and $I_W(i, j) = I_W$.




Original Image (I_0) | Watermark inserted (W) | Reconstructed watermarked Image (I_w) | Watermark Extracted (W')

Figure 3.


Median filtered Image | Extracted Watermark

Figure 4.


Cropped Image (25%) | Extracted Watermark

Figure 5.


Jpeg compressed image | Extracted Watermark

Figure 6.


Image after Bit compression | Extracted Watermark

Figure 7.

b) The robustness testing of the watermarked image:

The inserted watermark (W) and extracted watermark (W') must be exactly the same. The extent up to which this is achieved, is called normalized correlation coefficient (NC). Its value equal to unity indicates that W and W' are exactly same. Thus, NC=1 indicates perfect robustness of the algorithm. NC for watermark image W of size M×M is given by the following equation:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i.j) \times W'(i.j)}{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i,j) \times W(i,j)}$$

The calculated values of PSNR and NC after median filtering, image cropping, JPEG compression, bit compression and low pass filtering is given in table II.

Table 2: Values of PSNR and NC after different attacks

Attacks	PSNR(db)	NC
Bit compression	**39.6342**	**0.9123**
Image cropping	**42.4417**	**0.9317**
Median filtering	**40.5472**	**0.8324**
Jpeg compression	**37.0213**	**0.7756**
Low Pass Filtering	**40.5238**	**0.9021**

6 CONCLUSION

A secured image watermarking algorithm based on wavelet and compound encryption is discussed in this paper. Original watermark is pre-processed using cat mapping, logistic mapping and XOR function. Then the processed watermark is inserted into the desired wavelet channel and then the watermarked image is reconstructed. Then the watermark is extracted from the watermarked image. The watermarked image is then attacked by median filtering, Jpeg compression, bit compression and image cropping operations. After the attack, the values of PSNR and NC are calculated and compared. The experimental results support the claim of robustness and security of the proposed algorithm.

ACKNOWLEDGEMENTS

I sincerely thank Dr. Ramesh Vasappanavara, the Principal, R.A.I.T. for his guidance and support throughout the work.

REFERENCES

1. Yiwei Wang, John F. Doherty and Robert E. Van Dyck. “A wavelet-based watermarking algorithm for ownership verification of digital images”, IEEE trans.on image processing, vol.11, no.2, Feb.2002.
2. A. G. Bors and I. Pitas, “Image watermarking using DCT domain constraints”, proc. of IEEE Int. conf. on image processing, vol.3, pp 231- 234 (1996).
3. R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark”, proc. of Int. conf .on Image processing , vol.2, pp 86-90 (1994).
4. J. Ohnishi and K. Motsui, “Embedding a seal into a picture under orthogonal wavelet transformation”, Proc. of Int. conf. on multimedia comp. and system, p 514-521(1996-6).
5. D. Kundur and D. Hatzinakos, “A robust digital image watermarking method using wavelet based fusion”, proc. of IEEE Int. conf. on Acoustic, speech and signal proc. vol.5, pp 544-547 Seattle, Washington (1997-5).

6. R. Wolfgang and E. Delp, “A watermark for digital Image”, in proc. Int .conf. Image processing,vol.3, 1996, pp 211-214.
7. V. R. Dahake, N. R. Dasre, V. B. Gaikwad, “Digital watermarking in frequency domain using cat mapping”, Journal Of Science , Technology and Management, Vol-04, N0.-01, pp-11-16, (2011).
8. X. Y. Wang, “Chaos in the complex nonlinearity system”, Electronics Industry press, Beijing, 2003.
9. N. K. Pareek, P. Vinod , K. K. Sud, “Discrete Chaotic cryptography using external key”, Physics Letters A.2003, 309(2):75-82.
10. X. C. Wen, C. Jing, “An anti-statistical analysis LSB stenography, incorporating extended cat mapping”, Berlin Heidelberg, 2007, 12(5), 468-476.
11. G. FranQois, “Diffusion, approximation and Arnold cat map”, IEEE Transaction on Image Processing, 1996, 5(4):179-190.
12. Xie Jianquan, Xie Qing, Haungdazu. “The periodicity and security analyze of Arnold transform”, Computer security 2008, (5). 6-8.
13. Narendrakumar R. Dasre, Hemraj R. Patil “On watermarking in frequency domain”, proc. of SPIE-2010, vol.7546, 754622, 754622-1-5.