ISSN No. 0976-5697

Volume 4, No. 5, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Ownership authentication by using the combination of Arnold transformation and wavelet transformation in semi fragile watermarking

Seetaiah Kilaru
University of Birmingham, Department of Electrical Engineering, United Kingdom,
seetaiahkilaru@gmail.com

Yojana Kanukuntla
Electronics & Communication Engineering
Swarna Bharathi Institute of Science & Technology
Khammam
Yojanak5@gmail.com

Ramesh Garla
Electronics & Communication Engineering
Swarna Bharathi Institute of Science & Technology
Khammam
Rameshgarla497@gmail.com

Abstract: Watermark techniques are one of the traditional technologies to protect the information from illegal copying. It protects the authentication of the ownership rights. This paper proposes the semi fragile watermarking process which is robust and secure. In this algorithm, the combination of type-1 Discrete Wavelet Transformation and Arnold transformation was used to get the good Peak Signal to Noise Ratio (PSNR). The watermark is generated from the original image by obtaining low frequency LL sub band and embedded by using the High frequency sub band HH. The similarity ratio is measured to compare the original image and watermarked image quality. Results showed that, high quality is obtained even after the embedding process and robust against all common attacks.

Keywords: Semi-fragile watermarking, Arnold Transform, Peak Signal to Noise Ratio (PSNR) and Wavelet Transformation

I. INTRODUCTION

In current scenario, the definition of technology changed in a way that, it is best in areas of cost, simple and time efficient. Multimedia is one of the key elements which rules the world. The total world was digitized; even a toy that played by children also uses the DIGI technology. The main reason behind this one were fast processing rate and fast sharing of the data. This sharing may include normal data, secured data or any form of data. It is important to process the secure data in an efficient way without illegal occupancies. The patent owner may want to protect his data in a securable way. To do all these processes, digital water marking provides solution. This technique prevents unauthorized persons to manipulate original information. The application of this area includes digital books, drawings of engineering works and etc..

The existed image editing technologies are creating headache to the designers. Image tampering or forgery is also possible in digital transmission of data over unguided medium. Digital watermarking technique provides solution to all these problems. Digital watermark is nothing but a digital signature which tells information about the owner. In this process, the digital signature is embeds into the original image or message without changing any physical characteristics of the image. The effective watermarking technique has the qualities effective and robust against all attacks. There are two different watermarking approaches existed, they are

1. Visible watermarking
2. Invisible watermarking

The factor of invisibility depends on the factor of intensity. The invisibility and intensity factor are inversely proportional to each other. That means that better invisibility depends on the less intensity effect of the digital signature. The following are the characteristics for an effective watermark.

a. Unambiguous: In retrieval process of watermark, it has to identify unambiguously the owner.
b. Imperceptibility: The watermark should be invisible to human eye. If it visible, the attackers find it easily and they may try to delete it. If it is invisible, then it is difficult for them to find exactly where it is.
c. Robustness: the algorithm has to tolerate or has to unresponsive against all common attacks made by the different sources. It has to oppose all unnecessary transformations which try to change the image.
d. Quicker: the data owner can extract it in short span of time and with simple process.

The invisible watermark further classified into three types. They are

1. Robust
2. Fragile
3. Semi Fragile

Robust method: This method serves for the copy right protection. This method is designed especially to resist against lossy compression and predefined filter based operations. The processing operations does not involve any modification on embed watermark.

Fragile watermarking: This watermarking technique is considered as a sensitive process. In processing operation of an image, it does not allow even one bit image to change or modify. It is best suitable for the content authentication of an image.

Semi-fragile watermarking: the name itself indicates that, this method is fragile against some modifications and un

fragile against other modifications. For example, it may accept JPEG compression and didn't accept adding of any additive noise and tentative noise.

Importance of semi fragile: it is not possible to design fragile algorithm, because in defined circumstances, it may require to undergo some modifications. Along with this, it has to resist all other modification processes. Then by defining suitable algorithm which is in resist against some modifications and resist against remaining modifications.

It is possible to do this watermarking process in two different modes. They are

1. Spatial domain watermarking (SDW)
2. Frequency domain watermarking (FDW)

Spatial domain watermarking: In this process, the pixel undergoes certain modifications. This modification may use any transformation or user equation transformation. Out of all existing methods, Least Significant Bit (LSB) method is the best among all methods.

Frequency domain watermarking: in this process, the image is transformed into certain frequency range. After that all remaining modifications will apply to process the image. In this, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and several other methods are used in processing phenomenon.

Most of the watermarking techniques which are using now are insecure and low robustness. The proposed watermark method uses the DWT. In this process, watermark was generated from the spatial domain and embeds in the frequency domain. The effective combination of these two domains increased the robustness against attacks.

II. BACKGROUND

This background will explain about two key issues regarding the proposed scheme. They are DWT and Arnold Transformations.

Discrete wavelet transformation:

The given image will be divided into four different bands, namely LL, LH, HL and HH.

Here, the first letter describes about low/high pass frequency operation to rows and second letter shows the low/high frequency operation to the columns.

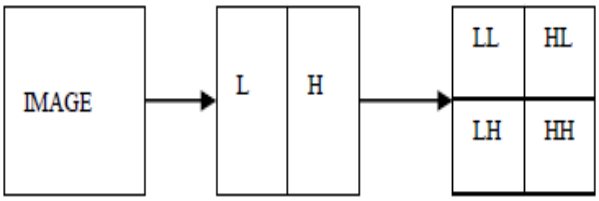

Fig1: decomposition of an image using DWT

The resolution of an image defined in four different parts. Out of all four, the LL sub band gives the approximate resolution level of an image. The remaining three parts will give the information about the detailed parts of an image.

LH defines about the vertical high frequencies, HL describe about the Horizontal high frequencies and HH defines about the all high frequencies.

For first level of decomposition the wavelet transformation for all these four sub bands are given as

$$LL = [(f(x,y) * \phi(-x)\,\phi(-y))\,(2n,2m)]_{(n,m)\in z^2}$$

$$LH = [(f(x,y) * \phi(-x)\,\psi(-y))\,(2n,2m)]_{(n,m)\in z^2}$$

$$HL = [(f(x,y) * \psi(-x)\,\phi(-y))\,(2n,2m)]_{(n,m)\in z^2}$$

$$HH = [(f(x,y) * \psi(-x)\,\psi(-y))\,(2n,2m)]_{(n,m)\in z^2}$$

Where Φ(t) represents the scaling function operated on lower frequencies and ψ(t) represents about wavelet baseband function.

Arnold transform:

This transformation is used to transform an image in scrambled way. This process adds security and creates confusion to the third party.

Let image function = f(x,y) = Z, where x,y ε (0,1,2,.N-1)

The image matrix can be changed into a new matrix by the Arnold transform which results in a scrambled version to offer security. It is a mapping function which changes a point (x, y) to another point (x1, y1) by

x' = (x+y) MODN

y' = (x+2y) MODN

III. PROPOSED METHOD

This method has 3 phases, like normal watermarking process. They are

1. Watermark generation
2. Watermark embedding
3. Watermarking extraction

In this process, we are not using external logo to embed the image. The watermark is generated from the information content of the original image. For the embedding process, it is recommended to use the type/level 1 DWT to be simple and fast. Here the main concentration to be put on HH band, because of its robust character.

Watermark generation:

- Take an original image of size M×M i.e host image = $I_{M\times M}$
- Compute the watermark from I such that watermark $I'_{M/2\times M/2}$
- Apply type-1 DWT and obtain $A_{M/2\times M/2.}$ From the four sub bands, obtain LL band.
- Maintain the block size as 2×2 and divide the original image into X number of blocks.
- Reduced image of size M/2×M/2 will be computed by taking one feature value from each above mentioned block. That value selection can be defined by the formula

$$B(x,y) = \frac{\sum_{j=1}^{2}\sum_{i=1}^{2} P(x*2+i, y*2+j)}{4}$$

Where $0 \le (x,y) \le M/2$

- Construct the image by using B(x,y) and consider it as K
- Calculate the difference between these two images (matrices) and consider it as L
- Let, define the value of W such that,

$$W(x,y) = \begin{cases} 0, & L \text{ is even} \\ 1, & otherwise \end{cases}$$

- Now, apply Arnold transform to get required watermark.

Watermark embedding:

The area to embed the watermark is the high frequency band, i.e. HH band.

- Obtain type/level 1 of DWT.
- Replace all HH1 components from the DWT with obtained watermark from above part.
- To obtain the watermarked image, apply inverse wavelet transformation.

Watermark detection:

In this process, we doesn't require original image in detection process. This type of watermark is called as blind watermark.

- Watermark is generated from the process described in generation.
- Apply DWT with type 1 and obtain HH1 sub band.
- Now compare the 2 values of DWT, if two values are matched each other, then authentication is preserved.
- If two values are not matched, then authentication is suspected.

IV. RESULTS

Consider the image with size 512Consider the image with size 512×512 image as follows.

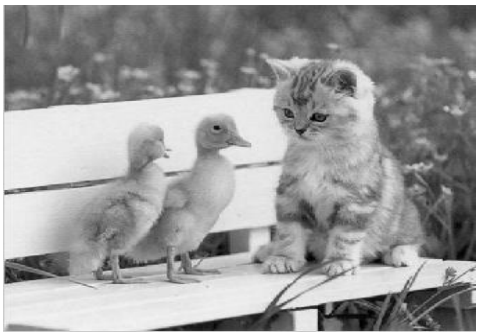

Fig2: original image

The constructed watermarked image as we described in the above process with half size 256×256 and it obtained as follows.

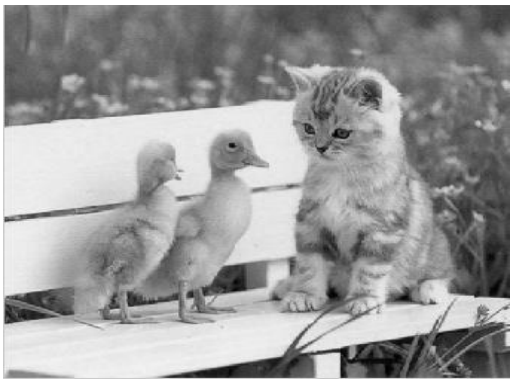

Fig: processed image (watermark)

The peak to signal ratio can be defined as

$$PSNR = 20 \log_{10} \frac{255}{MSE}$$

Where MSE can be defined as

$$MSE = \sum_{i=0,j=0}^{M-1N-1} \frac{[OI(i,j) - DI(i,j)]^2}{MxN}$$

Here OI represents the original image and DI represents the image with distortion.

The following table shows the performance against various attacks.

The performance factor between matched and distorted pixels is given by using Similarity Ratio (SR).

$$SR = \frac{S}{S+D}$$

Table1: value of SR under different circumstances

Attacks		SR
No		0.8259
Median filtering	3×3	0.6134
Linear filtering	3×3	0.6357
JPEG Compression	80	0.6234
scaling		0.7951

V. CONCLUSION

This paper explained about the novel watermarking methodology using semi fragile mode. Here, two bands are used instead of traditional one band concept. Low frequency band is used to generate the content based watermark and high frequency band is used in embedding process. This method also uses the Arnold transformation to confuse the third party. Finally, the algorithm is checked with the various noise attacks and results came quite satisfactory. The evaluation of this method best useful for the grey scale processing and still lot of scope existed in colour image

VI. REFERENCES

[1] K.L.Hung, C.C.Cheng, and T.S.Chen, "Secure Discrete Cosine Transform Based Technique for Recovereable Tamper Proofing", Opt Eng. 40(9), pp.1950-1958(2001).

[2] Xiang-Gen Xia, Charles G.Boncelet, Gonzalo: Wavelet Transform based watermark for digital images. In: OPTICS EXPRESS, 1998 Vol.3, No.12, pp 497-511.

[3] Sanjeev Kumar, Balasubramanian Raman, Manoj Thakur: Real Coded Genetic Algorithm based Stereo image Watermarking. In: IJSDIA, 2009, Vol. 1 No.1 pp 23-33.

[4] Hongmei Liu, Junhui Rao, Xinzhi Yao: Feature Based Watermarking Scheme for Image Authentication. In: IEEE, 2008, pp 229-232.

[5] J.Dittmann: Content-fragile Watermarking for Image Authentication. In: Proc. of SPIE, Security and Watermarking of Multimedia Contents III, vol.4314, pp.175-184, 2001.

[6] Rafael C.Gonzalez, R.E.Woods, , Steven L. Eddins : Digital Image Processing Using MATLAB, India (2008)

[7] Lin.C, Su.T and Hsieh.W, "Semi-Fragile Watermarking Scheme for Authentication of JPEG Images", Tamkang Journal of Science and Engineering, Vol.10, No.1, pp.57-66 (2007).

[8] Zhou.X, Duan X., and Wang D., "A Semi-fragile Watermark Scheme for Image Authentication", IEEE International Conference on Multimedia modeling, pp.374-377 (2004).

[9] C. Rey, J.Dugelay: A survey of watermarking algorithm for Image authentication. In: Journal on Applied Signal Processing, Vol.6, pp.613-621, 2002.

[10] C.I.Podilchuk, E.J.Delp: Digital watermarking: algorithms and applications. In: IEEE Signal Processing Magazine, pp. 33-46, July 2001.

[11] Arvind kumar Parthasarathy, Subhash Kak: An Improved Method of Content Based Image Watermarking. In: IEEE Transaction on broadcasting, Vol.53, no.2, June 2007, pp.468 -479.

[12] Ramana Reddy, Munaga V.N.Prasad, D.Sreenivasa Rao: Robust Digital Watermarking of Color Images under Noise Attacks. In: International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009.