Indian Journal of Science and Technology, Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/106816, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Improved Watermarking Technique for Image Authentication

Kausav Kumar* and Vineet Kumar

Department of Electronics and Communication Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India; kausavkumar23@gmail.com, vineet.15921@lpu.co.in,

Abstract

Digital image watermarking is one of the best techniques available now a day to tackle the problems regarding digital image authentication and its security. There are lots of ways and methods and techniques for digital image watermarking. This paper tried to improvise one of those techniques and comes up with a better and improved way to digital image watermarking. In this paper combination of two techniques: - Discrete Wavelet Transform and Arnold Transform are merged together in such a way that the outcome provides best possible results for invisible watermarking. Via using the new technique similarity ratio of 0.892 and signal-to-noise ratio of 59.11 is achieved. Technique is also measured against some of the common attacks on digital image.

Keywords: Arnold Transform, Discrete Wavelet Transform (DWT), Image Authentication, Invisible Watermarking, Signal-to-Noise Ratio (SNR), Similarity Ratio (SR)

1. Introduction

Latest technologies, latest mobiles, latest cameras, latest software etc. are launching every day. Same way their uses and misuses are also increasing day by day. Where latest camera technologies are used to take good and better quality digital pictures, at the same time new software are available to harm the integrity, security and privacy of those digital images which are nothing less than pieces of arts themselves. Some of those images represent happiest moments of someone's life, some represent someone's life work, some are proof of something, and some images are method of someone's earning, some are used for medical purpose and so on. There are so many uses of digital images in today's world that it is necessary to provide security to those images. There are lots of techniques which provide image security. Digital image watermarking is one of those techniques.

Digital image watermarking is a technique in which a person can leave his imprint on an image to assure its security. This imprint can either be a logo or some kind of digital signature or something else. The imprint can be visible or invisible or both as per the person's desire and requirement. On the basis of visibility digital image watermarking can be divided into two parts which are as follows:

1.1 Visible Digital Image Watermarking

In this watermarking the digital imprint on the image can be perceived by naked eyes. For example: a logo, signature etc.

1.2 Invisible Digital Image Watermarking

Digital imprint on the image cannot be seen with naked eyes in this type of watermarking. In this image, main goal is to apply the imprint in such a way that it's affect on image's visibility is as less as possible.

The biggest challenge of watermarking is to find the equilibrium between features such as robustness, safety and invisibility. Invisibility of watermark directly depends upon intensity of watermark embedded. Better invisibility is achieved from less intensity watermark. So, the minimum yet balanced intensity to embed a watermark in image is required. For robustness to increase it requires a stronger embedding, which in turn decreases the visual quality of an image.

*Author for correspondence

The main purpose of this paper is the invisibility of watermark embedded. The paper provides an algorithm for watermarking of image by combining two techniques.

- Discrete Wavelet Transform (DWT).
- Arnold Transform.

According to the paper, DWT is used to divide the image into four sub bands from which subband LL matrix is extracted. The second matrix is obtained by dividing the image into 2 X 2 non-overlapping blocks and finding the mean values of each block. The difference between two matrices is obtained and a new matrix is obtained. This matrix is then scrambled using Arnold Transform and the watermark is obtained. This watermark is then replaced with HH subband of the host image and watermarked image is obtained.

The remaining paper is organized as follows

Section 2 provides an overview of DWT, Arnold Transform. In section 3 watermark generation methodology, it's embedding and extraction is explained. Results are shown in section 4 and finally section 5 concludes this paper.

2. Related Background

This section explains the techniques used for producing watermark image which includes DWT and Arnold transform.

2.1 Discrete Wavelet Transform (DWT)

The DWT is used to decompose signal into approximation and detail. It is an implementation of wavelet transform using discrete set of the wavelet scales and translations obeying some defined rules. It provides sufficient information both for analysis and synthesis of the original signal, with a significant reduction in computation time. The DWT decomposes input image into four sub bands namely LL, HL, LH and HH.

The subband LL which is of lowest resolution level is the approximation part of the image. The remaining three sub bands contains the detail parts of image and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into the host image by replacing HH subband.

The 2D DWT of an image I (p, q) can be written as:

$$LL = [(I(p,q) * \varphi(-p)\varphi(-q))(2n, 2m)]_{(n,m)\in z^2}$$

$$LH = [(I(p,q) * \varphi(-p)\psi(-q))(2n, 2m)]_{(n,m)\in z^2}$$

$$HL = [(I(p,q) * \psi(-p)\varphi(-q))(2n, 2m)]_{(n,m)\in z^2}$$

$$HH = [(I(p,q) * \psi(-p)\psi(-q))(2n, 2m)]_{(n,m)\in z^2}$$

Where (t) is a low pass scaling function and (t) is the associated wavelet function.

2.2 Arnold Transform

Arnold transform is basically used for scrambling of an image. It is one of the basic techniques for digital image watermarking. In proposed algorithm, watermark obtained from host image is scrambled using Arnold Transform and then replace it with HH subband obtained by DWT of image. The image I (p, q) can be scrambled using following equation:-

$$\begin{bmatrix} p' \\ q' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} mod\ N$$

Where, (p, q) and (p', q') are the co-ordinates of image pixels before and after the Arnold Transform implementation.

3. Methodology

The paper proposes three significant steps for watermarking of an image.

3.1 Watermark Generation

As paper proposed earlier, the watermark is obtained from host image itself. The generation of watermark is proposed in two stages which are as follows

3.1.1 Stage 1

In this stage following two processes runs parallel to each other.

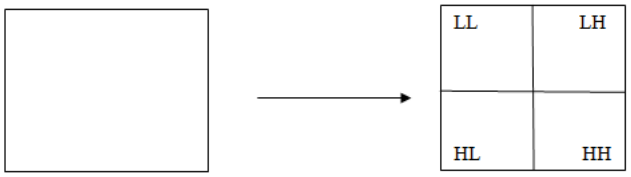

Figure 1. Original image of size N X N divided into 4 parts each of size N/2 X N/2 using DWT.

Process 1: There are following steps in this process.

- Take an image I (p, q) of size N X N.
- Now apply DWT on that image and divide it into four sub bands; each of size N/2 X N/2 and name them as LL, HL, LH and HH as explained in Section 2.1 and are shown in Figure 1

Process 2: This process has following steps

- Take the same image I (p, q) and divide the image into 2 X 2 non-overlapping blocks.
- Then mean value of each block is calculated using following Equation

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

- From these mean values a matrix B of size N/2 X N/2 is obtained.

After completion of these two processes the next stage of watermark generation begins.

3.1.2 Stage 2

This stage contains following steps:-

- Find the difference between LL and B matrices. Let this difference be C (where C is also of size N/2 X N/2).
- From here, obtain a new matrix of size N/2 X N/2 (let it be W) by using following Equation.

$$W(p,q) = \begin{cases} 1 & if\ LL > B \\ 0 & otherwise \end{cases}$$

- But sometimes due to calculations W matrix gets all its elements either 0 or 1. In this case, follow this Equation.

$$W(p,q) = \begin{cases} 0 & if\ C(p,q) is\ even \\ 1 & otherwise \end{cases}$$

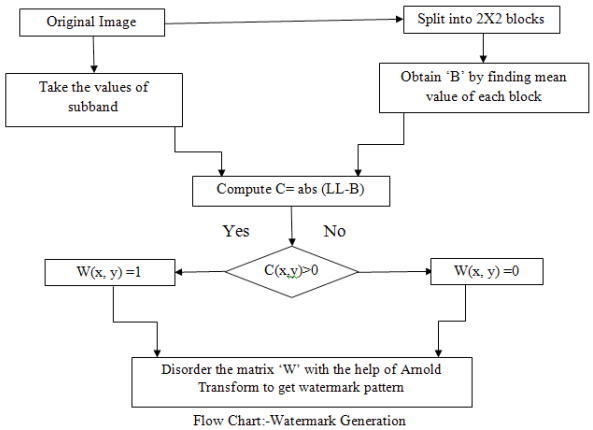

Figure 2. Flowchart- watermark generation.

Scramble the matrix 'W' with the help of Arnold Transform, the resultant matrix obtained is required watermark to be embedded in the host image.

3.2 Watermark Embedding

The high frequency subband of host image is replaced by watermark using following steps:

- Replace the HH subband of image with W matrix.
- Apply inverse DWT on remaining 3 portions (LL, HL and LH) and W matrix.
- A new image obtained is the required watermark image.

3.3 Watermark Extraction

The watermark is extracted from original image using following steps:

- Apply 2D DWT to the watermarked image and extract HH subband of watermarked image and replace it with the HH subband of original image.
- Compare the two watermarks (derived and extracted). If the values matched that means authenticity of image is preserved else it is suspected.

4. Results

An image of size 128 X 128 is taken which is shown in Figure 3. The image contains equal No. of rows and columns due to implementation of Arnold Transform. A watermark of size 64 X 64 is generated from image itself as explained in Section 3.1. The generated watermark is embedded into the image via using technique explained in Section 3.2 and a watermarked image is generated as shown in Figure 4. The difference of original image and watermarked image is shown in Figure 5. This difference in both images confirms a very high level of fidelity.

Figure 3. Orginal image.

Figure 4. Watermarked image.

Figure 5. Difference image.

Various types of attacks were applied on watermarked image to test its robustness. Gaussian Noises of factor (0, 0.01) and (0, 0.001) were added to the watermarked image. In the same fashion Salt and Pepper noise of factor 0.002 was applied to watermarked image.

Some other types of common attacks were also applied on watermarked image. For example: The old intensity values of watermarked image are shifted to new values such that 1% of data is saturated at low and high intensities. Two types of filtering were also applied to the image: 1. Linear Filtering 2. Median Filtering. Attacks like blurring and rotation (5^o and 10^o) were also applied on same image. Some other attacks were also applied on same image which are shown in Table 1.

The visual quality of both watermarked and attacked images is measured using the Peak Signal to Noise Ratio, which is defined in equation below. The PSNR value of watermarked image is 59.1168, which signifies that there is very little distortion in the quality of original image.

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)$$

Where, MSE is Mean Square Error between original image and distorted image defined in following Equation.

Table 1. Assessment of PSNR and SR

Attacks		PSNR(db)		Similarity Ratio	
		Method	Proposed	Method	Proposed
Adding Gaussian (mean, variance)	0, 0.01	32.8092	38.3272	1	0.8371
	0, 0.001	30.0730	30.0997	0.5188	0.5042
Adding Salt & Pepper Noise	0.002	32.0513	32.1381	0.9898	0.8370
Median Filtering	3 x 3	29.5819	29.5727	0.5218	0.6629
Linear Filtering	3 x 3	27, 2292	27.7761	0.5359	0.6696
Image Adjustment		18.7003	18.5312	0.8433	0.8435
Blurring		37.8281	37.8322	0.6712	0.8083
Histogram Equalization		19.0192	19.0944	0.7573	0.7598
JPEG (quality factor)	90	43.013	43.1448	0.4659	0.6488
	70	36.4452	37.4799	0.4753	0.6956
	50	35.2058	35.4799	0.4745	0.7418
	30	33.1859	33.2002	0.4759	0.7736
	10	29.1818	29.1867	0.4746	0.8158
Scaling		51.0944	56.1065	0.4985	0.8463
Rotation	5°	13.9478	13.9492	0.5071	0.7135
	10°	12.0324	12.0325	0.4648	0.6957

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

Where OI (i, j) is original image and DI (i, j) is distorted or watermarked image of order M X N.

Similarity Factor is measurement of the similarity of pixel intensities between the original image and the watermarked image. If SM = 1 then the embedded watermark and the extracted watermark are same. Generally value of SM > 0.75 is accepted as reasonable watermark extraction. Extracted and original watermark can be compared by computing Similarity Ratio (SR) between these two patterns as defined in equation given below.

$$SF = (\sum_i \sum_j OI(i,j) * DI(i,j)) / \sum_i \sum_j DI(i,j)^2$$

By using above Equation, SM comes out is 0.9034 which is above required limit.

5. Conclusion

This paper has introduced a new and improved watermarking technique for digital images. This paper provides complete algorithm for embedding and extracting watermark efficiently and effectively. In this algorithm the watermark embedded is extracted from the host image itself and that watermark is scrambled with the help of Arnold Transform. Then that watermark is embedded into the host image in such way that there is no degradation in the visibility (visual quality) of the image. The algorithm uses Discrete Wavelet Transform (DWT) for providing a frequency spread of watermark in the image. The obtained watermarked image is evaluated with some of the common image processing attacks like filtering, histogram equalization, image compression, rotation, and image scaling, Gaussian noises and Salt and Pepper noises. The results show that the image's security is robust against those types of attacks. Moreover the algorithm provides authentication as well as imperceptibility to the image.

6. References

1. Rajawat M, Tomar DS. A secure watermarking and tampering detection technique on rgb image using 2-Level DWT. IEEE 5th International Conference on Communication Systems and Network Technologies; 2015.
2. Qi X, Xin X, Chang R. Image authentication and tamper detection using two complementary watermarks. Computer Science Department. UT 84322-4205; 2009.
3. Mangroliya S, Pathak K. Tamper localization in wavelet domain using semi-fragile watermarking. IJEDR. 2014; 2(2). ISSN: 2321-9939.
4. Lin SD, Lin JH, Chen C-Y. A ROI-based semi-fragile watermarking for image tamper detection and recovery. ICIC International. 2011 Dec; 7(12).
5. Chahal JS, Khurana S. Digital image watermarking using spread spectrum technique under DWT domain. IJERT. 2014 Mar; 3(3). ISSN: 2278-0181.
6. Yang C-K, Huang C-S. A novel watermarking technique for tampering detection in digital images. Electronic Letters on Computer Vision and Image Analysis. 2004; 3(1):1–12.
7. Li K-F. Chen T-S, Wu S-C. Image Tamper Detection and Recovery System Based on Discrete Wavelet Transformation. 2001 IEEE Pacific Rim Conference on Communications, Computers and signal Processing; 2001.
8. Tsai M-J, Chien C-C. A wavelet-based semi-fragile watermarking with recovery mechanism. IEEE International Symposium on Circuits and Systems; 2008.
9. Yuping H, Guangjun G. Watermarking-based authentication with recovery mechanism. 2nd International Workshop on Computer Science and Engineering; 2009.
10. Som S, Palit S, Dey K, Sarkar D, Sarkar J, Sarkar K. A DWT-based digital watermarking scheme for image tamper detection, localization, and restoration. India: Springer; 2015.