Secured & High Resolution Watermarking Technique

Charu Kavadia[1], Vishal Shrivastava[1], Mayank Pokharna[2]
[1]*Department Computer Science Engineering, Arya College of Engineering & I.T.Jaipur (Raj.), India*
[2]*Department of Electronics & Communication, CTAE, MPUAT, Udaipur (Raj.), India*
charukavadia@gmail.com

***Abstract*— the watermarking is a method of embedding some king of hidden authentication information with cover image so that it can be identified later. There are many methods available which uses some kind of signal or the binary images, however sometimes it is difficult to defend that the recovered signal/image is same embedded watermarked image because there is always a possibility to get similar patterns form non watermarked images, hence in this paper we presents a secure watermark technique which is capable to embed 8 bit image. The experimental results shows that the technique is not only time efficient but also immune to different attacks.**

Keywords: Digital watermark, discrete wavelet transform, chaotic encryption.

*****

I. Introduction

Everyday tons of data is embedded on digital media or distributed over the internet. The data so distributed can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. These challenges motivated researchers to carry out intense research in the field of watermarking. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of the same concept [1]. There are two types of watermarks: visible watermark and invisible watermark. In this paper we have concentrated on implementing invisible watermark in image. The main consideration for any watermarking scheme is its robustness to various attacks. Watermarking dependency on the original image increases its robustness but at the same time we need to make sure that the watermark is imperceptible [2].

II. Literature Review

The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some selected pixels is called the LSB embedding technique [6]. The watermark is actually invisible to human eyes. However, the watermark can be easily destroyed if the watermarked image is passed through filters or compression. To increase the security of the watermark, Matsui and Tanaka [3] proposed a method that uses a secret key to select the locations where a watermark is embedded, e.g. the use of a pseudo-random number generator to determine the sequence of locations on the image plane. J.Samuel Manoharan et al [4] in their focused towards studying the behavior of Spatial and Frequency Domain Multiple data embedding techniques towards noise prone channels and Geometric attacks enabling the user to select an optimal embedding technique. Keshav S Rawat et al [5] presents the survey on digital watermark features, its classifications and applications. Various watermarking techniques have been studied in detail in mainly three domains: spatial, frequency and statistical domain. In spatial domain, Least-Significant Bit (LSB), SSM-Modulation-Based Technique has been developed. For DCT domain, block based approach and for wavelet domain, multi-level wavelet transformation technique and CDMA based approaches has been developed. Their work also presents the various error matrices for analyses the robustness of watermarking method. B Surekha et al [7] In their paper, three public image watermarking techniques are proposed. The first one, called Single Watermark Embedding (SWE), uses the concept of Visual Cryptography (VC) to embed a watermark into a digital image. The second one, called Multiple Watermarks Embedding (MWE) extends SWE to embed multiple watermarks simultaneously in the same host image. Finally, Iterative Watermark Embedding (IWE) embeds the same binary watermark iteratively in different positions of the host image, to improve the robustness. Experimental results show that the proposed techniques satisfies all the properties of digital watermarking such as invisibility, security ,capacity, low computational complexity and is robust to wide range of attacks.

III. DWT (Discrete Wavelet Transform)

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time).
The DWT is computed by successive low pass and high pass filtering of the discrete time-domain signal as shown in figure 1. This is called the Mallat algorithm or Mallat-tree decomposition. Its significance is in the manner it connects the continuous time mutiresolution to discrete-time filters. In the figure, the signal is denoted by the sequence x[n], where n is an integer. The low pass filter is denoted by G0 while the high pass filter is denoted by H0. At each level, the high pass filter produces detail information; d[n], while the low pass filter associated with scaling function produces coarse approximations, a[n].

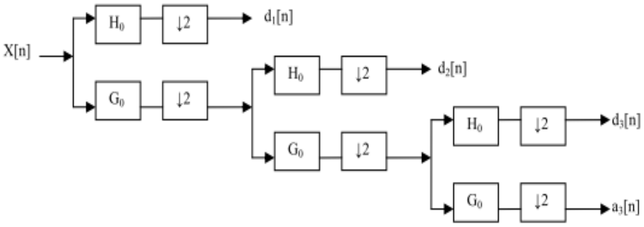

Figure 1: Three-level wavelet decomposition tree.

The agreement adopted by many DWT-based watermarking methods, is to embed the watermark in the middle frequency coefficient sets is better in perspective of imperceptibility and robustness .

IV. DCT (Discrete Cosine Transform)

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. With an input image, x, the DCT coefficients for the transformed output image, y, are computed according to Equation.1 shown below. In the equation, x, is the input image having N x M pixels, x (m, n) is the intensity of the pixel in row m and column n of the image, and y (u, v) is the DCT coefficient in row u and column v of the DCT matrix.

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_m\alpha_n\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left\{x(m,n)\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)u\pi}{2N}\right\}$$

.... (1)

Where

$$\alpha_u = \begin{cases}\frac{1}{\sqrt{2}} & for\ u = 0\\ 1\ for\ u = 1,2,\ldots,M-1\end{cases}$$

$$\alpha_v = \begin{cases}\frac{1}{\sqrt{2}} & for\ u = 0\\ 1\ for\ v = 1,2,\ldots,N-1\end{cases}$$

The image is reconstructed by applying inverse DCT operation

$$x(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_m\alpha_n\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left\{y(m,n)\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)u\pi}{2N}\right\}$$

V. 5. Arnold's Cat Map

Arnold's Cat Map is a transformation that can be applied to an image. The pixels of the image appear to be randomly rearranged, but when the transformation is repeated enough times, the original image will reappear. For digital square image, discrete Arnold mapping can be achieve by using following equation.

$$\binom{x}{y} = \left[\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\binom{x}{y}\right] mod\ N$$

The values of square matrix used in above equation can be used as key so that only same matrix can reverse the encryption.

VI. Proposed Algorithm

The proposed algorithm can be described in the steps described below.

Step 1: Perform DWT on the host image to decompose it into four non-overlapping multi-resolution coefficient sets: LL1 , HL1 , LH1 and HH1 .

Step 2: Perform DWT again on two HL1 and LH1 coefficient sets to get eight smaller coefficient sets and choose four coefficient sets: HL12, LH12, HL22 and LH22.

Step 3: Perform DWT again on four coefficient sets: HL12, LH12, HL22 and LH22 to get sixteen smaller Coefficient sets and choose four coefficient sets: HL13, LH13, HL23 and LH23.

Step 4: Divide four coefficient sets: HL13, LH13, HL23 and LH23 into 4 x 4 blocks.

Step 5: Perform DCT to each block in the chosen coefficient sets (HL13, LH13, HL23 and LH23). These coefficients sets are chosen to inquire both of imperceptibility and robustness of algorithms equally.

Step 6: scramble the watermark signal with Arnold algorithm for key times and gain the scrambled watermark Ws (i, j), key times can be seen as secret key.

Step 7: Perform inverse DCT (IDCT) on each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 8: Perform the inverse DWT (IDWT) on the DWT transformed image, including the modified coefficient sets, to produce the watermarked host image.

VII. Experimental Results

For the testing of the proposed algorithm following measures are used for assessment of quality of image and watermark.

Peak signal-to-noise ratio (PSNR) & Mean Squared Error (MSE):

PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

It is most easily defined via the mean squared error (MSE) which for two mXn monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

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

$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

The proposed algorithm has been extensively tested on various standard images.

Table I summarizes the watermarking results.

Figure 2: Test images Barbara, Baboon, and Peppers

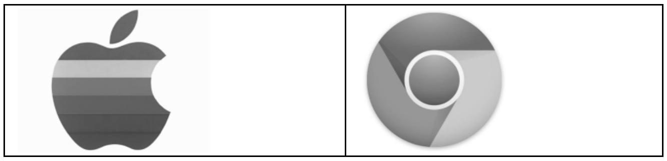

Figure 3: images used for watermarks

Table 1: Experimental results for non-attacked case

Image	MSE	PSNR(dB)
Baboon	58.90	30.42
Barbara	69.08	29.73
Peppers	62.11	30.19

Table 2: Experimental results for watermark embedding & retrieval time (image size 256x256) non-attacked case.

Image	Embedding Time (Sec.)	Retrieval Time(Sec.)
Baboon	0.0761	0.021
Barbara	0.0655	0.018
Peppers	0.0738	0.022

Gaussian Noise Attack

Table 3: Experimental results for Gaussian Attack (mean = 0.0, variance = 0.05)

Image	MSE	PSNR(dB)
Baboon	17219	5.77
Barbara	18954	5.35
Peppers	16592	5.93

Scaling Attack

Table 4: Experimental results for Scaling Attack

Attack	Image	PSNR(dB)
Scaling(50%)	Barbara	12.08
	Baboon	14.11
	Peppers	14.69
Scaling(75%)	Barbara	11.77
	Baboon	12.80
	Peppers	13.76

JPEG Compression Attack

Table 5: Experimental results for JPEG Compression Attack (CPR = 2)

Image	MSE	PSNR(dB)
Baboon	736.0254	19.46
Barbara	899.8828	18.88
Peppers	653.7695	19.97

VIII. CONCLUSION

The simulation results shows that the proposed method give very good results and the it is robust to many types of attack (as the table above shows), the results also shows that the embedding and retrieving time for watermark in the proposed technique is also very low and hence proves the technique is quite fast. The robustness in the test shows that the PSNR of the watermark after compression attack remains above 18 dB and with scaling attack it remains above 11db which is quite recognizable when we are using 8 bit image.

IX. REFERENCES

[1]Santi Prasad Maity, Malay Kumar Kundu “Robust and Blind Spatial Watermarking in Digital”Image”http://www.isical.ac.in/~malay/Papers/ Conf/ICVGIP_02_WM.pdf.

[2]R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital watermark", Proceedings of IEEE International Conference on Image Processing, Vol. 1, 1994, pp. 86-90.

[3]Darshana Mistry “Comparison of Digital Water Marking methods”, International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2905-2909.

[4]Keshav S Rawat, Dheerendra S Tomar “Digital Watermarking Schemes For Authorization Against Copying or Piracy of Color Images”, Indian Journal of Computer Science and Engineering Vol. 1 No. 4 295-300.

[5]Sviatoslav Voloshynovskiy, F. Deguillaume, Shelby Pereira and Thierry Pun “Optimal adaptive diversity watermarking with channel state estimation” University of Geneva - CUI, 24 rue du General Dufour, CH 1211, Geneva 4, Switzerland.

[6]B Surekha, Dr GN Swamy “A Spatial Domain Public Image Watermarking“International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011.

[7]John N. Ellinas “A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection” World Academy of Science, Engineering and Technology 34 2007.

[8]Xiaojun Qi “An Efficient Wavelet-Based Watermarking Algorithm”