

An Enhanced Digital Watermarking for Color Image using Support Vector Machine

Dr.Yogendra Kumar Jain ,Saurabh Tiwari
 Computer Science & Engineering Department,
 Samrat Ashok Technological Institute, Vidisha, (M.P.), India.

Abstract - In this paper, we have proposed an improved & logistic digital watermarking scheme, which collected based on Support Vector Machine (SVM) for color image. The watermark is embedded into the discrete wavelet domain of the original image and extracted by training support vector machine, which have the component of the image. For performance enhancement of support vector machine, we consider the adding of momentum coefficient to reduce the error and increase the rate of the learning. The watermark can be successfully extracted by training the support vector machine, and the (SVM) watermarking algorithm is good for many kinds of common attacks. The experimental results reveal that the proposed algorithm can achieve the desired result and high stoutness to general image processing technique & geometric distortion.

Keywords: Digital watermarking, Discrete wavelet transform, Support vector machine (SVM), color image.

1. INTRODUCTION

The digital information provides a great convenience for the depositing, adopting and using to information. The development of computer network communications make information exchange and transmission becoming relatively simple and quick, but digital image, audio and video products [3] such as multimedia digital copyright-protected security questions in such a communications environment are also increasingly exposed.

The Internet is an open network, being increasingly used for delivery of digital multimedia contents. In the digital format, content is expressed as streams of ones and zeros that can be transported flawlessly. The contents can be copied perfectly infinite times. A user can also manipulate these files. However, good business senses necessitates two transaction mechanisms content protection and secure transport over the Internet. The content protection mechanism attempts to protect the rights of the content creator, distributor and user. The content owner deposits a unique description of the original to a neutral registration authority. This unique distribution may be hash value or textual description. Now, the registration authority allots a unique identification number to the content and archives these two for future reference. This unique identification number is also conveyed to the content owner.

Business of online delivery and distribution via CD/removable disks of multimedia products face huge obstacles due to unlimited perfect copying and manipulation at the user end. Digital watermarking is

the technology used for copy control, media identification [6], tracing and protecting content owner's rights.

In related research, several spatial domain watermarking schemes have been proposed. The color quantization [1] scheme, proposed an approach for image watermarking by modifying the color index table. When the pixel mapping procedure for color quantization is performed, the watermark is embedded at the same time. But, to enhance the robustness of the scheme, the distribution of colors in the palette of host image must be uniform. Consider human visual effects to adaptively adjust the embedding watermark bits. The number of watermark bits for embedding in this scheme is determined by the visual effect of the pixel values in the host image [2] propose a method based on amplitude modulation. In their method, robustness is improved by multiply embedding a watermark and adaptive threshold for extracting from two reference watermark bits. The idea of amplitude modulation is further developed by combining SVM in [4]. Propose an SVM-based color image watermarking algorithm. The watermark bits and additional 1024 training bits are embedded in the blue channels of pixels. For extraction phase, the 1024 embedded training bits are employed as training samples of the SVM. When the SVM is trained, it is used for extracting the watermark.

2. RELATED WORK

Intelligent systems are being used in several different fields. In watermarking, it is being applied successfully at different watermark stages such as embedding, detection and decoding. Recently, in watermarking work have used self-governing Component Analysis to extract watermark correctly without using the original image. Correctness of the watermarking Extraction depends on the key and the statistical independence between the original image and the watermark. Have introduced an watermark decoding scheme. This scheme performs SVM based supervised learning. Have illustrated the application of SVMs as discriminative models [10] for the refined search spaces. They have shown that SVMs can be used for continuous speech recognition. In work have used the idea of perceptually shaping the watermark with respect to both the conceivable attack and cover image at the embedding stage. Information pertaining to watermarked cover coefficients and conceivable attack is utilized. A watermarked data can be attacked in different ways. However, each application usually has to deal with a particular set of distortions. Some of the attacks are addition of Gaussian and Non Gaussian noise, signal processing attacks like D/A conversion, color reduction, linear

filtering attacks like high pass and low pass filtering, lossy compression, geometric distortions etc. Keeping in view the expected distortions, different approaches like redundant embedding, selection of perceptually significant coefficients, spread spectrum modulation, and inverting distortion in the detection phase are investigated to make a watermark system reliable.

3. SUPPORT VECTOR MACHINE

SVM has emerged in recent years as a popular approach to the classification of data. SVM is [8] margin-based classifier with good generalization capabilities. It is the method of creating functions from a set of labeled training set given by

$$S = \{ (x_i, y_i) \mid x_i \in R_n, y_i \in \{1,-1\}, i=1,\dots,m \}$$

Where x_i stands for input vector i and y_i is the desired category, positive or negative, SVM can generate a separation hyper plane H that separates the positive and negative examples. Since SVM has the maximum generalization

Ability to separate data into two classes, thus it is naturally suitable for detecting a given bit to be zero or one (watermark bit). If any point x which lies on the hyper plane must satisfy $w \cdot x + b = 0$, where w is normal to the hyper plane and b is the bias. Finally, the optimal hyper plane $H: w \cdot x + b = 0$ can be determined by

$$w_0 = \sum \alpha_i y_i x_i$$

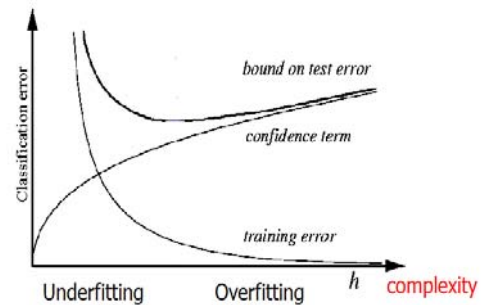
where α_i and b_0 are Lagrange multipliers and bias that determined by SVM's training algorithm. In Eq., those points x_i with $\alpha_i = 0$ can be ignored and those with $\alpha_i > 0$ are called "support vectors". After the training of SVM is completed, H is thus determined, then any data x will be classified according to the sign of the decision function. The decision function is defined as:

$$d(x) = \text{sgn} (\sum \alpha_i y_i K(x_i, x) + b_0)$$

Where $K(x_i, x)$ is the kernel function which maps the training samples to a higher dimensional feature space. The function can be either a classification function or a general regression function. SVM finds an optimal separating hyper-plane between data points of different classes in a high dimensional space. Support vectors are the [9] points that form the decision boundary between classes. SVM decoding models are based on the Structural Risk Minimization (SRM) principle from statistical learning theory. Different SVM classification models have been selected due to their high discrimination power and low generalization error.

SVM is powerful to approximate any training data and generalizes better on given datasets. The complexity in terms of kernel affects the performance on new datasets. SVM supports parameters for controlling the complexity and above all SVM does not tell us how to set these parameters and we should be able to determine these

Parameters by Cross-Validation on the given datasets. The Graph given below gives a better illustration.



SVM are based on statistical learning theory. They can be used for learning to predict future data. SVM are trained by solving a constrained quadratic optimization problem. SVM, implements mapping of inputs onto a high dimensional space using a set of nonlinear basis functions. SVM can be used to learn a variety of representations, such as neural nets, splines, polynomial estimators, etc, but there is a unique optimal solution for each choice of the SVM parameters. This is different in other learning machines, such as standard [5] Neural Networks trained using back propagation. In short the development of SVM is an entirely different from normal algorithms used for learning and SVM provides a new insight into this learning. The four most major features of SVM are duality, kernels, convexity and sparseness.

SVM decoding models can be developed by using different kernel functions. Two issues are catered in order to optimize SVM models, i.e. selection of suitable kernel function and its associated parameters (model selection) [7]. In optimal kernel selection, first, SVM are tested on various kernels for improved classification performance and minimum training

Error. In kernel model selection, mostly iterative search is applied in order to optimize the parameters within a specified range. In the current work, we are optimizing different SVM kernel functions in the decoding of message bits in watermarking.

Support vector machine training

On the training of SVM, the water mark is extended and embedded into the original image. We assume that the water mark W is binary and consists of two Sequences T and S as: $W = TS = t_0 t_1 t_2 \dots t_{N-1} s_0 s_1 s_2 \dots s_{M-1}$. The first binary sequence $T = t_0 t_1 t_2 \dots t_{N-1}$ denotes the training information of length N which is generated by pseudo- random number generator (PRNG) with seed1. In our experimental, N is equal to 128. The sequence $S = s_0 s_1 s_2 \dots s_{M-1}$. Represent the owner's digital signature of length M . It may be a binary sequence or a binary image (logo). The binary sequence of water mark is shown in figure 2.

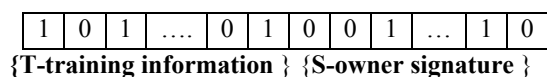


Fig 1 binary sequence of a water mark

Steps of algorithm:

1. Begin
 2. Training Information Embedding
- For $I = 0$ to $\tilde{N}1$

3. Compute the luminance L_{pi} at position P_i by the follow equation:

$$L_{pi} = 0.299R_{pi} + 0.587G_{pi} + 0.114B_{pi}$$

R_{pi} , G_{pi} , B_{pi} , represented, red, green and blue channel values of the pixel at P_i position.

4. The training information bit t_i is embedded into the host image by modifying the blue channels B_{pi} and B'_{pi} , at positions P_i and its 4-neighbors P_i according to the luminance L_{pi}

$$B_{pi} = B_{pi} + \alpha(2t_i + 1) L_{pi} \quad \alpha = 0.15$$

$$B'_{pi} = B'_{pi} + \alpha(2t_i + 1) L_{pi} \quad \alpha = 0.05$$

Where α is a positive constant that determines the Watermark strength,

When position P_i is selected, its surroundings should not be selected again. If any of surrounding position is selected, then the value of B'_{pi} will be re-modified that may cause the inaccuracy in the retrieval phase. After training information T is embedded.

A. Watermarking Embedding

The watermark embedding process transforms the original image into the wavelet domain. The tests are performed on the 256x256 Lena Baboon, fort and pepper images as the original watermark images. The proposed watermark embedding algorithm is summarized as follows:

1. Split the original image I into blocks with the size of $g \times g$ and perform the three-level DWT transformation on each block. Select the position of watermark embedding coefficient using random sequence.
2. Create the better-quality support vector machine and initialize its parameters, we use T as supervised signal and the average value of each block is used as the desired output value of the SVM to train SVM. In this experiment, the training error is set to be 0.001.
3. Training enhanced support vector machine using input and output values, and the watermark is embedded into the wavelet domain using the trained SVM.
4. Perform the inverse discrete wavelet transform (IDWT) on the coefficients where the watermark is embedded to obtain the watermarked image.

B. Watermarking Extraction

The watermark extracting procedure is inverse procedure of watermark embedding, the steps are as follows:

- 1) Perform the three-level DWT transformation on the watermarked image blocks.
- 2) Select the position of coefficient $C(i, j)$, where watermark is embedded with the same secret key which used in watermark embedding sequence. Quantize the DWT coefficient by Q , and use it as input value of the trained SVM to get the output T .
- 3) Extract the watermark Calculate the Correlation between the original watermarks And the extracted watermark to detect the Existence of the watermark.
- 4) The mean squared error (MSE) will be used

$$MSE = \frac{1}{N} \sum (I_i - I_j)^2$$

$$N = 0$$

4. EXPERIMENTAL RESULT

For the entire test, we have taken Matlab version 7.0. A digital watermarking technique based on support vector machine for color images has been proposed in this paper. In our experiments, we use the 256x256 Lena fig2(a), Baboon fig3(a), Fort fig4(a), Pepper fig5(a) color images as the original images for all the tests shown in Fig.2 (b) and Fig3(b), then Fig4(b) and 5(b) are the watermarked images. The watermark is a 32x32 logo image, for all the image taken for watermarking process the image quality of the watermark image is coming out to be greater than 40, PSNR, value above 30 db indicates that image quality is good the watermark image and original images cannot be traced with simple observation .

- 1) Lena – the popular image Lena has be taken by us for first experiment, as shown in table we having 40.83db PSNR value which indicate the successful embedding of watermark. Similarly for other image..

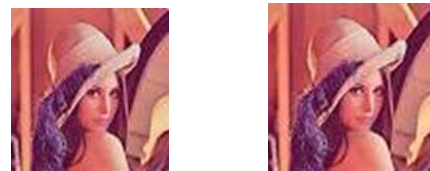


Fig 2(a) original image, Fig 2 (b) watermark image

Table I: Watermark Lena image against attack psnr (db)

S.NO.	ATTACK	MSE	PSNR(db)
1	Attack Free	61.45	40.83
2	Gaussian noise	230.18	33.09
3	Salt noise	737.14	26.264
4	Poisson noise	912.75	25.011
5	Multiplicative noise	1220.50	23.308

- 2) Baboon



Fig 3(a) original image, Fig 3(b) watermark image

Table II: Watermark Baboon image against attack psnr (db)

S.NO.	ATTACK	MSE	PSNR(db)
1	Attack Free	38.98	43.499
2	Gaussian noise	252.21	32.55
3	Salt noise	678.226	26.75
4	Poisson noise	814.77	25.677
5	Multiplicative noise	1024.10	24.33

3) Fort



Fig 4(a) original image Fig 4(b) watermark image

Table III: Watermark Fort image against attack

S.NO	ATTACK	MSE	PSNR(db)
1	Attack Free	50.177	42.01
2	Gaussian noise	251.25	32.57
3	Salt noise	704.32	26.53
4	Poisson noise	882.28	25.21
5	Multiplicative noise	1183.61	23.48

4) Pepper



Fig 5(a) Original image Fig 5(b) Watermark image

Table IV: Watermark Pepper image against attack

S.N O.	ATTACK	MSE	PSNR (db)
1	Attack Free	61.86	40.79
2	Gaussian noise	232.67	33.025
3	Salt noise	787.62	25.87
4	Poisson noise	947.13	24.79
5	Multiplicative noise	1239.94	23.21

5) Result Comparison: The comparison shows that the proposed scheme has better performance than traditional neural network approach against all type attack, so support vector machine is a superior tool for watermarking.

Table V: Comparison with BPN

PSNR(db) COMPARISON				
Images	Lena	Baboon	Fort	Pepper
Our method	40.83	43.49	42.01	40.79
Traditional BPN	40.21	42.1	41.20	40.34

5. CONCLUSION

In this paper, a watermarking algorithm has been projected with support vector machine for color image. SVM the capability to learn the characteristics of the image, and the watermark is embedded and extracted by the trained SVM. Updating the weights with adding momentum coefficient to train the SVM we can attain an optimum estimate to a given network target. We embed the watermark into DWT using the support vector machine, which can reduce the error and improve the rate of the learning, and the watermark can be well extracted. Experimental results show that the proposed method has good imperceptibility and high strength to common image processing such as JPEG compression, noise adding, chopping, and rotation.

REFERENCES

- [1] J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions Image Process*, vol.6, no.12, pp.1673-1687, December 1997.
- [2] M.D. Swanson, M. Kobayashi, A.I-1. Tewfik, "Multimedia data embedding and watermarking technologies," *Proc. IEEE*, vol.86, no.6, pp.1064-1087, June 1998.
- [3] Masataka Ejima, Akio Miyazaki, and Taku Saito, "A wavelet-based watermarking for digital images and video," In *proceedings of the IEEE International Conference on Image Processing, ICIP '00*, Vaneouver, Canada, September 2000.
- [4] J.R. Hernandez, M. Amado, and F. Perez-Gonzalez, "OCT-Domain watermarking techniques for still image: Detector performance analysis and a new structure," *IEEE Trans. Image Processing*, vol.9, pp.55-68, January 2000. 3117
- [5] Jian Zhao, Qin Zhao, Ming-quan Zhou, and Jian-shou Pan, "A Novel Wavelet Image Watermarking scheme Combined with Chaos Sequence and Neural Network, Advanees in Neural Networks," *Lecture Notes in Computer Science*, Springer-Verlag, Berlin Heidelberg, vol.3174, pp.663668,2004.
- [6] P Moulin, M K Mihcak. A Framework for Evaluating the Data-Hiding Capacity of Image Sources [J]. *IEEE Trans. on Image Processing*, 2002, Vol. 11, No.9:1029~1042.
- [7] H.-H. Tsai, C.-C. Liu and H.-C. Tseng, "SVM-based lossless image watermarking," *Information Security Conference*, Chiayi, R.O.C., 2007.
- [8] C.J.C. Burges, "A Tutorial on support vector machines for pattern recognition," *Data Min. Knowledge Discovery*, pp. 121–167, 1998
- [9] Y.Fu, R.Shen and H.Lu, 'Watermarking scheme based on support vector machine for colour images', *IEE 2004, Electronics Letters*, 5th August 2004 Vol. 40 No. 16.
- [10] J. He, H. Hu, R. Harrison, P. C. Tai, and Y. Pan, "Transmembrane segments prediction and understanding using support vector machine and decision tree," *Expert Syst. With Appl. (Special Issue on IntelligentBioinformatics Systems)*, vol. 30, no. 1, pp. 64–72, Jan. 2006