

Svm Classifier Enabled Quad Tree Segmentation For Adaptive Image Watermarking System

Ruban R¹, Dr.S.SanthoshBaboo²

*Assistant Professor, Head of The Department of BCA & MSC Computer Science
ST.Josephs college Arts & Science, Kovoor.¹*

*Associate Professor, DwarakaDossGoverdhanDoss VaishnavCollege, Chennai.²
rubanlrs@gmail.com¹, Santhos1968@gmail.com²*

Abstract

In the image watermarking system, the actual values of the carrier image data are modified according to some kind of rules; carrier image and watermark image can be perfectly restored without any change on the receiver side. Generally there is lot of inference (attacks) causes, during the retrieval of watermark image. To tackle those kinds of attacks, in this paper, we propose an SVM classifier based Quad Tree Segmentation (SVM-QTS) methodology. Here binary image act as a watermark image and RGB image plays as a carrier image. We perform QTS on carrier image by manipulate SVM classifier, which allocates the sufficient space to hide a watermark image. Additionally, we analyzed the overall performance of SVM-QTS methodology under some kinds of attacks.

Index Terms: Watermarking digital image, Quad Tree Segmentation, Support vector machine, PSNR, Successful Retrieval.

Introduction

Generally, digital watermarking is referred as a kind of sign embedded through the multimedia data like image, audio, video contents in a covert environment manner. Due to the rapid proliferation of multimedia based online services, researchers direct towards digital data. It is often, utilized to recognize tenure of the copyright of such multimedia data. "Watermarking" is the event of embed digital data over a transporter signal; the concealed in sequence should subsistence, but doesn't coherence to the carrier signal or cover image.

Attackers of either the stored or transferred data designed to present copyrighted material, as their own belongings. Embedding based digital watermarking methodology offers competent tool for ensuring that content ownership of these multimedia is preserved even if multimedia data is processed by such attackers.

It is notably used for tracing copyright infringements and for banknote verification. Like square watermarks, digital watermarks are only visible below firm circumstances, i.e. after using several algorithm, and indiscernible anytime else. If a digital watermark deforms the carrier signal in a way that it happens to be perceivable, it is of no use. Traditional Watermarks may be pertained to perceptible medium (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models.

Many of the watermark embedding processes is executed in either spatial domain or change domain. In spatial field watermarking scheme [1] the watermark image is unswervingly embedded into the host image by altering its pixel values. Both the insertion and extraction methods are fairly simple compared to transform domain watermarking schemes. Nevertheless, it is more complicated for spatial domain watermarks to attain imperceptibility because of the need to entrench high intensity digital watermark for robustness leans to disgrace the image visual quality.

Transform domain methods [2] & [3] are vigorous as contrasted to spatial domain schemes. This is due to the reality that when image is inverse transformed, watermark is disseminated intermittently over the image, making the attacker complex to read or modify. Due to the actuality of localization in cooperation spatial and frequency domain, wavelet transform is the mainly preferable transform amongst all other transforms.

Dawei et al. proposed a innovative type of technique in which the authors used the wavelet transform applied locally, based on the chaotic logistic map [4]. This method shows very excellent stoutness to geometric harass but it is sensitive to common attacks like filtering and sharpening.

Xinpeng Zhang et.al proposed an original fragile watermarking method capable of entirely receiving better the original image from its interfered version. Bits and check-bits are established into the host figure by a lossless statistics beating method. On the receiver side, by estimate the extracted and calculated check-bits; one can categorize the tampered image-blocks [5]. Hongjie et.al presented the performance analysis of a "self-recovery fragile watermarking scheme" [6] using block-neighbourhood tamper characterization. This technique uses a pseudorandom sequence to create the nonlinear block-mapping and employs an optimized neighborhood characterization technique to notice the tampering.

Despite the wide variant of usages and applications, a good watermark should possess some common characteristics such as imperceptibility, robustness, security, reliability and low computation cost. In recent years, efforts have been made to take advantage of machine learning techniques for watermark embedding and extraction.

Yu et al proposed a digital watermarking method in spatial domain based on artificial neural networks (ANNs), where employing multi-layer perceptions (MLPs) calculated adaptively its thresholds [7]. Chang et al presented a robust DWT-based copyright verification scheme with fuzzy-ART, which combines DWT, fuzzy-ART and the quantization process [8]. Support vector machines (SVMs), as a new class of machine learning methods based on statistical learning theory, can overcome over-fitting weakness of neural networks.

Related Works

Yu-Chi Liu et.al have proposed an adaptive DE-based reversible steganographic scheme [9] with bilinear interpolation and simplified location map is proposed. In conventional reversible difference expansion (DE) method, it undergoes two troubles: the embeddable position is deemed inadequate and the embedding payload control capacity in single layer embedding is feeble. For the primary problem, the kernel of bilinear interpolation is applied to efficiently progress the number of the embeddable location while the value of the stegoimage can be maintained at a good level. [10] Xinpeng Zhang et.al have proposed a novel self-embedding watermarking method based upon a reference partaking mechanism, in which the watermark to be embedded is a reference derived from the unique principal content in different regions and shared by these regions for content reinstatement. A self-embedding method proficient of reinstating the watermarked image from a interfered edition were briefly discussed.

Lin et.al have proposed a DRM system protects and impose the rights connected with the use of digital content. Regrettably, the technical challenges for protecting digital content are redoubtable and previous moved have not succeeded. They outline the notions and approaches for video DRM and explain processes for providing security, counting the roles of encryption and video watermarking [11].

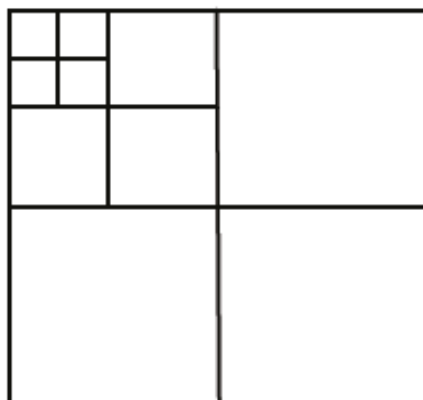


Figure 1: Quad-tree subdivision

Cheng-Hsing Yang et.al have proposed a novelty based adaptive least-significant bit (LSB) steganographic method using pixel-value differencing (PVD) that provides a larger embedding capacity and imperceptible stego images. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels. Pixels located in the edge areas are embedded by a -bit LSB substitution method with a larger value of than that of the pixels located in smooth areas [12]. Wien Hong has proposed a reversible data embedding method based on histogram shifting and achieved an excellent embedding performance. Their method shifts the absolute difference of two consecutive pixels for data embedment, and employs an embedding level to control the payload. However, the shifting of

absolute difference reduces the number of embeddable spaces and results in a reduction in payload [13].

The quad-tree technique employs the well-known image processing technique depends upon a recursive splitting of selected image quadrants, enable the resulting partition to be represented by a tree structure in which each non-terminal node has four descendants. The partition is made by selecting an initial level in the tree (equivalent to a number of greatest range block size) and recursively partitioning any block for which a match better than some preselected threshold is not found. Compact coding of partition information is possible by taking benefit of the tree structure of the partition [14]. The method made here combines a quad-tree smoothing practice with arithmetical classification performed at the maximum level of the quad-tree, followed by a downward directed boundary estimation based on the segments obtained at the top level of the tree. The quad-trees have many applications such as image segmentation, data smoothing, edge enrichment and image compression. Also for the manipulation of image complication and in some cases it is used for extracting features [15].

Proposed SVM-QTS Methodology

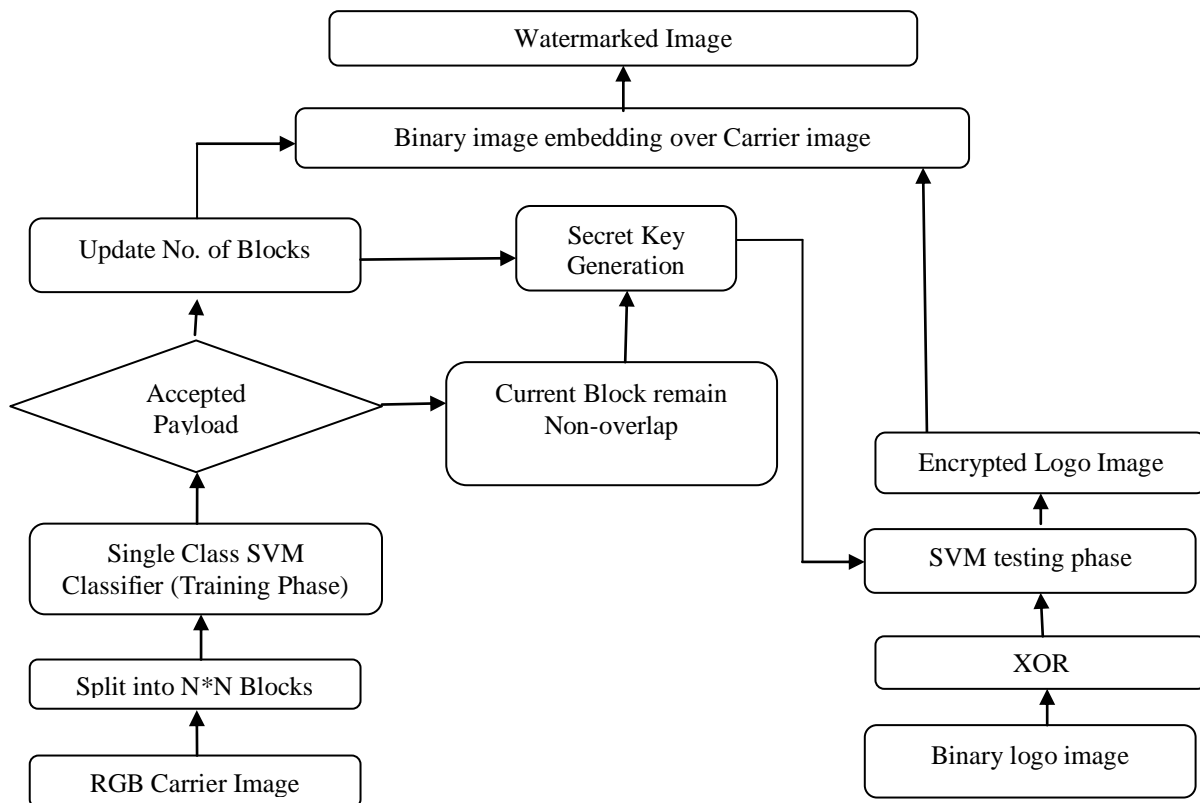


Figure 2: Detail flow chart of SVM-QTS based Image watermarking

In the future methodology, we develop image watermarking system based on gray scale and binary combination. According to the doing well recovery of both carrier image and watermark image; following process plays such an significant role indexing, classification, clustering and so on. We manipulate SVM classifier to perform QTS-Quad Tree Segmentation technique for image watermarking. The preprocessing step of SVM train phase, host image is split into several non-overlapping blocks and payload calculation for each block. After the difference calculation among total payload and external payload, whenever testing situation got satisfied go ahead with sub splitting process in iterative manner.

SVM based Quad Tree Segmentation (SVM-QTS)

SVM has been efficiently pertained to various organization and prototype acknowledgment difficulty. SVM is maintained to lead improvised simplification properties. Recently most of the researchers have been prefer Support Vector Machine classifier for digital watermarking. A quad-tree is a tree data structure in which each inside node has exactly four blocks (from initial split n*n blocks). These blocks are created through split the face representation and planned as a design of quad-tree formation. Here gray scale illustration select as a carrier reflection and binary image act as a watermark image. In QTS segmentation process the initial step of SVM train phase begins here. Single set SVM classifier decide whether the current block split into sub-blocks or not, with deference to the payload variation between the carrier and watermark image. The process is continued until all the block partitions are negotiated.

The cover image "C" is divided into several non-overlapped blocks c_1, c_2, \dots, c_n . Calculation of secret data's payload followed by

$$PS_{sec}(C) = h(M_1) - (\log N)^2 * h(m_1) - 16 \dots \dots \dots (1)$$

$$PS_{tot}(C, P) = \sum_{i=1}^P h_i(M_{i,1}) - (\log N)^2 \times \sum_{i=1}^P h_i(m_{i,1}) - P \times 16 \dots \dots \dots (2)$$

Here, $(M_{i,1}, m_{i,1})$ is stands for combination of greatest and least amount points of the i^{th} image block and $h_i(x)$ stand used for histogram of the i^{th} image block. Here we need to estimate the payload combination over each incoming block.

SVMs are easier and better to use than conventional neural network models. The idea of SVM is to assemble a rising scheme from input info to output info which is also defined as features for input info and targets for output info.

SVM Train Phase

SVM classifier perform block wise validation according to the following either or conditions. Single class SVM often provides the logical and reasonable decision like true or false to develop QTS over both the carrier image and watermark image. From eq,1&2, we can evaluate the payload calculation (PS_{tot} & PS_{sec}).

If the underground image payload is greater than the total payload size, then-current block is evenly sliced into four blocks $(c_{i,1}, c_{i,2}, c_{i,3}, c_{i,4})$. This means preceding block not ready to embed the corresponding watermark block. In spite of a reverse, cases just make it the current block as remains constant (ci), so capable of embed the corresponding watermark block.

SVM test phase and watermark embedding

During SVM test phase, we generate the secret key as the bit-stream. Bit-stream is the collection of binary information. Whenever the delivery service image block is sliced into four blocks, bit stream key value printed as 1 else 0. Hereafter watermark image, were encrypted successfully with respect to the bit-stream key value.

Successfully the space was allocated over a carrier image; by manipulate single class SVM classifier. According to secret and carrier image, non overlapped blocks have been prepared successfully. During embedding phase, double representation merges over a cover image without disturbing the actual pixel values of the carrier image. SVM classifier plays such an important role to achieve our goal.

Performance Evaluation

After successful embedding of watermark image over carrier image. Its mandatory to analyze overall performance even at the recipient end, because various kinds of attacks degrade the watermarked image quality. Hence, there is a possibility to make an impact over the successful retrieval of both watermark and carrier image. We consider the subsequent well known image watermarking attack, brighten, darken, salt and interrupt noising. To estimate the performance of SVM-QTS methodology, we take the following images as input to our system.

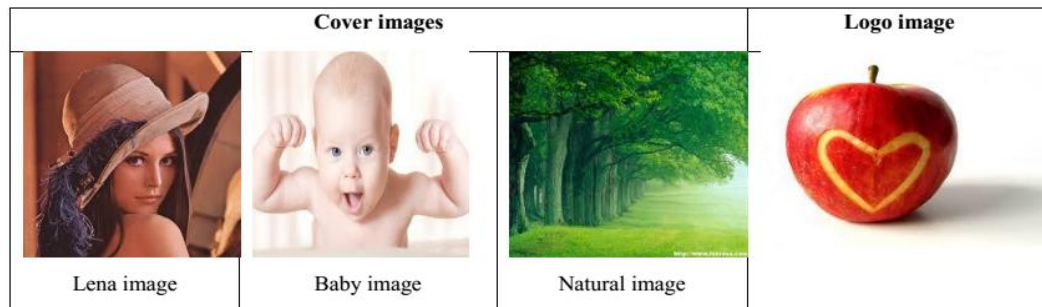


Figure 1: List of carrier images and watermark image utilized during performance check

Results Table [SVM]

Table 1: PSNR Comparison of Various Attacks For SVM_QTS Method

Attack	PSNR [Baby Image]	PSNR [Nature Image]	PSNR [Lena Image]
No Attack	55.8922	55.906	55.8717
salt & pepper	36.6679	34.454	35.2019
Painting	30.5995	39.0399	34.5571
Brighten	55.1417	55.1196	55.0818
Darken	55.0891	55.1406	55.1716

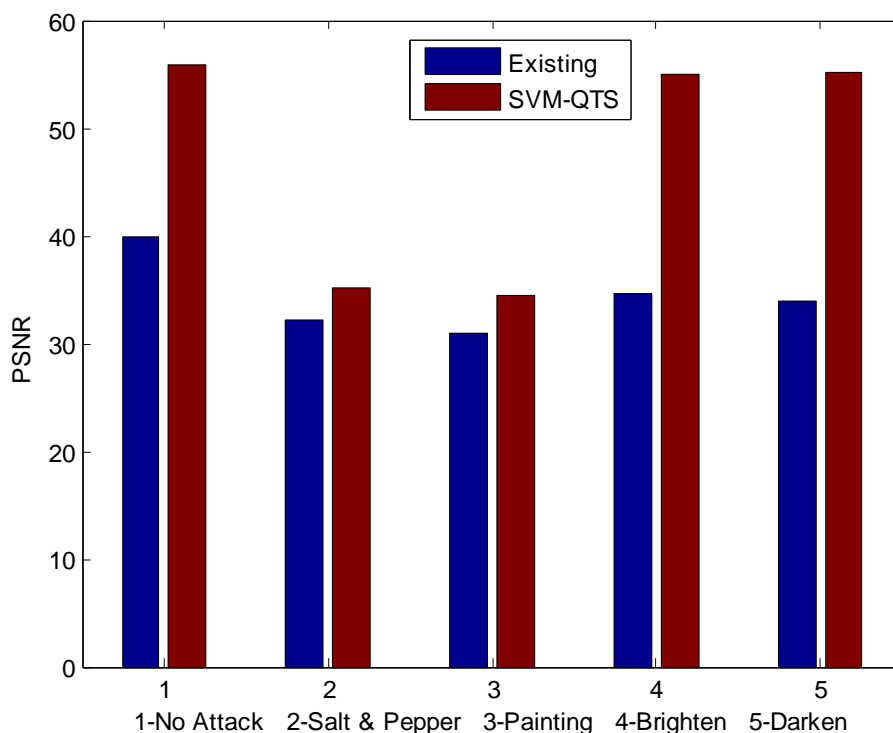


Figure 2: Comparison result of Existing and SVM-QTS methodology

Brightening attack:

We apply the brighten attack, by summing a +ve constant to the luminance of each pixel over the whole watermarked image. After the brightening of the watermarked image, the image becomes authentic.

Darkening Attack:

We apply darkening attack, by subtracting a +ve constant starting the watermarked image pixels. Darken the watermarked image will cause, visible to the naked eyes and easy to retrieve the watermark image.

Painting Attack:

By physically, we paint over the watermarked image. Paint attack is capable for scaling the images. The watermarked image will be downscaled and it will be extracted.

Salt and pepper attack:

The common attack used on watermark image is salt and pepper attack. Salt and pepper noise often occurs in images due to imperfect memory locations. The effect of salt and pepper noise is similar to a Gaussian noise attack since it increases the variation in pixel values in spatial domain.

Conclusion and Future Work

In this paper, we developed an efficient and robust image watermarking system named "SVM_QTS based image watermarking methodology". We elect the MATLAB R2012a as a simulation tool, to implement our proposed methodology. SVM classifier act as a bridge between the watermark image and carrier image. During SVM training phase meanwhile, we generate the bit-stream based binary format secret key. This generated secret key posses the integrity of the watermark representation, due to the bit-stream key act as an encryption key. in addition, we successfully retrieved the watermark image under different kinds of attacks. We direct our future work as combination of image watermarking system with neuro-fuzzy technique.

References

- [1] R. G. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in Proc. IEEE Int. Conf. Image Process., vol. 2, Nov. 1994, pp. 86–90.
- [2] C. Rey and J. L. Dujelay, "Blind detection of malicious alterations on still images using robust watermarks," in Proc. IEE Secure Images and Image Authentication Colloquium, London, U.K., Apr. 2000, pp. 7/1–7/6.
- [3] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," in Proc. Int. Congress IPR for Specialized Information, Knowledge and New Technologies, Vienna, Austria, Aug. 1995, pp. 242–251.
- [4] Z. Dawei, C. Guanrong, L. Wenbo, A chaos based robust wavelet domain watermarking algorithm, Chaos, Solitons, and Fractals 22 (2004) 47–54.
- [5] Xinpeng Zhang and Shuozhong Wang, "Fragile Watermarking With Error-Free Restoration Capability",IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 10, NO. 8, DECEMBER 2008.
- [6] Hongjie He, Fan Chen, Heng-Ming Tai, Ton Kalker, and Jiashu Zhang,"Performance Analysis of a Block-Neighborhood- Based Self-Recovery Fragile Watermarking Scheme",IEEE transactions on information forensics and security, vol. 7, no. 1, february 2012 185.
- [7] Yu, P.-T., Tsai, H.-H., Lin, J.-S., 2001. Digital watermarking based on neural networks for color images. Signal Processing 81, 663–671.
- [8] Chang, C.-Y., Wang, H.-J., Pan, S.-W., 2009. A robust DWT-based copyright verification scheme with fuzzy-ART. Journal of Systems and Software 82, 1906–1915.
- [9] Yu-Chi Liu, Hsien-Chu Wu and Shyr-Shen Yu, "Adaptive DE based reversible stegano graphic technique using bilinear interpolation and simplified location map", Springer Science+Business Media, Multimed Tools Appl (2011) 52:263–276 DOI 10.1007/s11042-010-0496-0.
- [10] Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng,"Reference Sharing Mechanism for Watermark Self Embedding",

IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 2, FEBRUARY 2011 485.

- [11] eugene t. Lin, ahmet m. Eskicioglu, reginald l. Lagendijk and ahmet m. Eskicioglu, reginald l. Lagendijk, "Advances in Digital Video Content Protection", PROCEEDINGS OF THE IEEE, VOL. 93, NO. 1, JANUARY 2005.
- [12] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, and Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", iee transactions on information forensics and security, vol. 3, no. 3, september 2008.
- [13] Wien Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting", Optics Communications (Elsevier) 285 (2012) 101–108.
- [14] Fatemeh Alamdar and MohammadReza Keyvanpour, "A New Color Feature Extraction Method Based on QuadHistogram", Elsevier, Procedia Environmental Sciences, Vol.10, 2011.
- [15] Yuanhai Shao, Wei Chen, Chan Liu, "Multiwavelet based Digital Watermarking with Support Vector Machine Technique", IEEE, 2008, pp. 4557-4561.

23008

Ruban R