Robust Digital Watermarking Using MDKP

Mr A. Chandra, Ms. T. Kavitha

Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College,
A.Rangampet, Tirupathi, India

Abstract- The growth of digitalization of data creates a need for protecting digital content against counterfeiting, piracy and malicious manipulations. Digital water marking is one of the methods of protecting multimedia data. A robust digital watermarking method is proposed in this paper, which has greatest robustness against various attacks and preserves the image quality after water marking. It embeds a watermark into an image in DCT domain. The image is divided into blocks and each block is processed using Multi Dimensional Knapsack Problem (MDKP) and in turn converts to spatial domain. The watermark is extracted from the image and compared with the original image. The measurement of quality of image is also concerned. The proposed scheme exhibits better performance in robust digital watermarking. The experiment is carried using MATLAB 7.x and results are verified.

Index Terms- Copyright protection, Digital Watermarking, DCT, MDKP

I. INTRODUCTION

Digital technologies have grown dramatically and widely used within home computers and open networks. Digital content is volatile and easily processed. Digital objects may be modified easily without any control. Digital watermark is a piece of information embedded into potentially vulnerable images in such a way it is in separable from the image.

The digital watermarks can be divided into three different types as visible watermark, Invisible-Robust watermark, and Invisible-Fragile watermark. Visible watermark is a transparent object overlaid into the primary image. The watermark will be visible to a casual viewer on a careful observation. The invisible-robust watermark is embedded in such a way that changes made to the pixel value are not noticed, which can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any alternations of the image would alter or destroy the watermark [3].

Several applications of watermarking have been considered by researchers [2]:

Copyright: In this case, the mark is associated with an identity number. In this way, the mark identifies the owner of the content and can be used for copyright purposes (prevent illegal copies). The embedding and the detection of the mark depend on a secret key. The mark has to be robust and detectable after numerous processing treatments or attacks that preserve the original content.

Database Retrieval and Data Hiding: In this case, the mark permits the identification of the content. The mark contains a description of the content or a pointer to this description and can be used for database "classification." In this application, the robustness of the mark is not decisive but the mark has to be detected after basic format conversion.

Authentication: The mark can be a fragile mark that will disappear after image manipulation. It can be used to authenticate the content and to prove that its integrity has been preserved. The function of the mark is to prove that the content has not been manipulated and consequently the robustness of the marking algorithm is not a prior achievement.

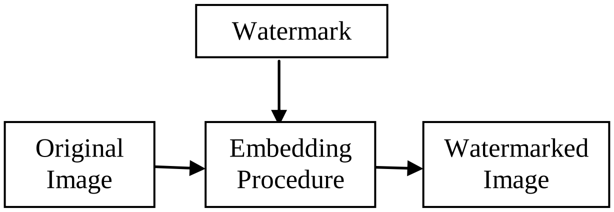

Figure 1: Block Diagram of Watermarking

Attacks which attempt to destroy or invalidate watermarks can be classified into two types, noise-like signal processing and geometric distortions. Noise like signal processing is intended to remove embedded water marks from the cover image by a signal processing approach. Geometric distortion makes a detector fail to detect the existence of watermark even if they are still on the image. Geometric distortions can be resisted by transform-based, pilot-based and feature-based schemes [1].

Watermark can be inserted into the image using various techniques like spread spectrum and feature based techniques. Insertion and detection of watermark using the above techniques consumes too much computation time. As a result, we propose a method of inserting watermark into image using MDKP in DCT domain to reduce the computation time. The cover image is divided into blocks and an MDKP is formulated to optimize the selection of most robust blocks in the image. Watermark is inserted into the blocks by transforming them to DCT domain. After insertion of watermark they transformed back to spatial domain. The experimental results is applied to some images the proposed method will have better robustness than existing methods.

The paper is organized as follows. Various watermarking schemes are described in section II. Proposed watermarking scheme using MKDP in DCT domain is described in section III and concluding remarks is made in section IV.

II. RELATED WATERMARKING SCHEMES

Several previous digital watermarking methods have been proposed. In [4], the authors propose a scheme for watermarking images. The method breaks up an image into 8×8 block and computes a DCT to each of these blocks. A pseudorandom subset of the blocks is chosen, then, in each such block, a triple of frequencies is selected from one of 18 predetermined triples and modified so that their relative strengths encode a one or zero value. The 18 possible triples are composed by selection of three out of eight predetermined frequencies within the 8 × 8 DCT block. The choice of the eight frequencies to be altered within the DCT block is based on a belief that the "middle frequencies...have moderate variance," i.e. they have similar magnitude. This property is needed in order to allow the relative strength of the frequency triples to be altered without requiring a modification that would be perceptually noticeable.

Chih-Wei Tang and Hsuesh-Ming Hang [5] propose a scheme that takes original image; the feature extraction method which generates reference centers of disks for watermark embedding and detection. Then it performs the image normalization technique on disks in the original image. The coordinate transformation coefficients between the original image disks and the normalized ellipse images are generated. The location of blocks in the original image for watermark embedding is determined from the normalized image. Then, coordinates of selected points are transformed from normalized image back to the original image. Next, a 2-D FFT is applied to these 32×32 blocks on each qualified disk in an original image. The watermark is embedded in the transform domain. Last, the watermarked blocks are 2-D IFFT converted back to the spatial domain to replace the original image blocks. The drawback of this scheme is watermark resistance is low for severe geometric distortions.

Jin S. Seo and Chang D. Yoo [6] propose a procedure that constructs invariant regions at each scale from the scale space Harris points of an image; selects invariant regions for watermarking, considering the spatial positions and the repeatability measures. Watermark is embedded additively into the selected regions after geometric normalization according to the shape of the regions.

Jen-Sheng Tsai, Win-Bin Huang and Yau-Hwang Kuo [1], in this scheme a region set is obtained by a feature detector. Here the algorithm works in two phases. During the primary feature set searching stage, watermark is inserted into the detected feature regions and secondly simulated attacking is performed. By analyzing the attack resistance of the regions primary feature set is identified. On which genetic algorithm based feature set solution is done to resist undefined attacks. There are several drawbacks of this scheme. Only predefined attacks can be simulated and algorithm consumes too much computation time robustness of feature regions due to simulated attacking.

The existing techniques are generally resistant to various attacks but consume more computation time. The proposed method is a secure digital watermarking scheme and is a faster robustness measurement scheme.

III. WATERMARKING USING MDKP

One of the major difficulties for watermarking is that watermark embedding and detection should be performed over the same blocks of an image. The flow diagram of the scheme shown in fig 2. Watermark is embedded into the original image in DCT domain using MDKP. Extraction of watermark is also implemented.

A. Implementation of Work

We propose an algorithm which works in DCT domain using MDKP. The algorithm uses the DCT block size as 2×2. The original size of the image considered in the experiment is 64×64. The image is processed into blocks; the blocks are transformed using DCT.

The symbol g_b^a is defined to indicate the overall resistance degree of the block *b* against attack *a*. It is determine by

$$g_b^a = \left(d_{b,a_1} + d_{b,a_2} + \; \dots + d_{b,a_{Na}}\right) = \sum_{i=1}^{N_a} d_{b,a_i} \qquad (1)$$

Where $d_{b,a_i} \in \{0,1\}$, indicates if block *b* can resist the i^{th} predefined attack a_i and N_a is the total number of predefined attacks. The symbol g_b^c indicates the property related to corner response of the block *b*. It is zero, if it is less than threshold is set to 1% of the maximum response value. We use binary symbol g_b^g to indicate whether region belongs to the middle scale band or not. This can be formulated into an MDKP as [8]

$$\text{maximize } \sum_{j=1}^{n} (\; g_{b_j}^a + g_{b_j}^c + g_{b_j}^g) S_{b_j} \qquad (2)$$

subjected to

$$\sum_{j=1}^{n} w_{k,b_j} s_{b_j} < c_k \; k = 1,2 \dots\dots n \; S_{b_j} \qquad (3)$$

is defined as

$$S_{b_j} = \begin{cases} 1, \text{ if the block } b_j \text{ is selected} \\ 0, \text{ otherwise.} \end{cases} \qquad (4)$$

The variables w_{k,b_j} and c_k represent the composite weights and constraints of quality distortion and overlapping conditions. This MDKP is solved for determining the best choice of blocks.

Insert watermark into the block, transform block back into spatial domain and move on to the next block, and write the watermarked image out to a file. Finally separate the watermark from the image using DCT block size. Compare the watermark extracted image to the file compare it with the original image. If the change is less than threshold then the image is not distorted.

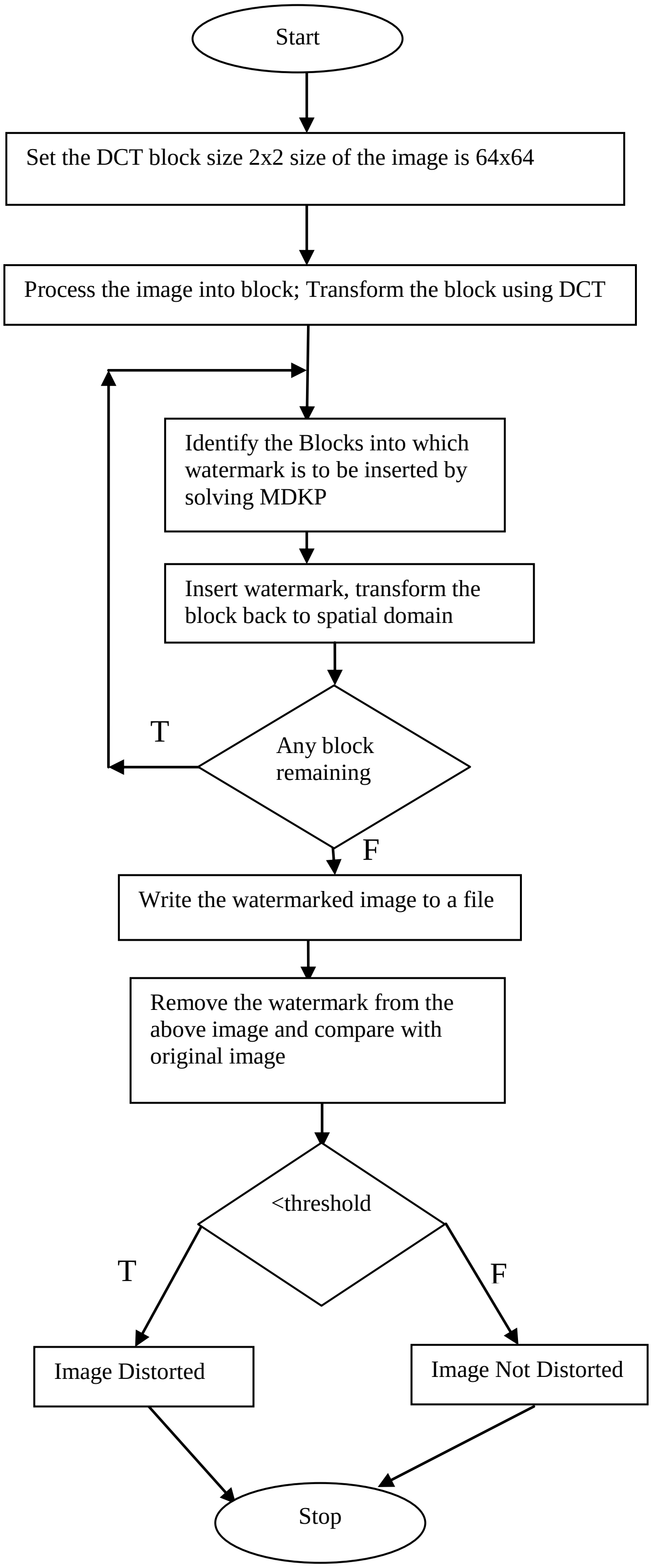
Start
Set the DCT block size 2x2 size of the image is 64x64
Process the image into block; Transform the block using DCT
Identify the Blocks into which watermark is to be inserted by solving MDKP
Insert watermark, transform the block back to spatial domain
Any block remaining
T
F
Write the watermarked image to a file
Remove the watermark from the above image and compare with original image
<threshold
T
F
Image Distorted
Image Not Distorted
Stop

Figure 2: Flow diagram of the proposed scheme

B. Experimental Results and Analysis

The experiment is carried on various images viz. lena, babbon, and pepper.

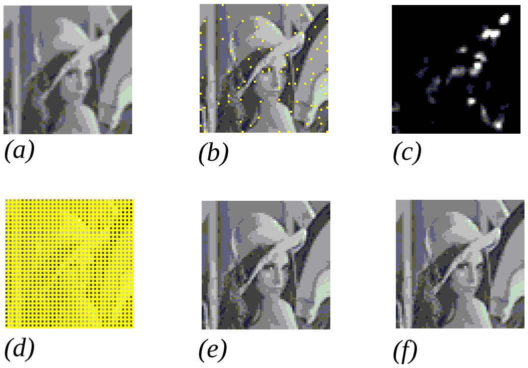

Figure 3: Image changes in the proposed scheme

Here (a) is 64×64 lena image taken for the experiment. The corner point's response of the image is generated in (b). To know the attack resistance analysis the corner metric response of image is taken which is shown in (c), with the help of the corner point's and corner metric responses are used for dividing the cover image into 2×2 blocks of the image(d) to transform using DCT. The watermarked image(e) and the watermark extracted image(f) is shown, physically no difference is observed between (e) and (f) because invisible watermarking[9] scheme is used.

Iteration time in seconds of the algorithm for selecting 2×2 blocks of the various images is shown in table 1.

Table 1: Iteration history

Lena	Baboon	Pepper
0.000444515	0.00058403	0.000481004
0.000444515	0.00058403	0.000456938
0.000444515	0.00042494	0.000456938
0.000444515	0.00042494	0.000456938
0.000325351	0.00042494	0.000456938
0.000325351	0.00042494	0.000456938
0.000325351	0.00042494	0.000456938
0.000325351	0.00042494	0.000456938
0.000325351	0.00042494	0.000456938

The proposed scheme consumes less time compared to the method proposed in [1] for lena image is shown in the graph below.

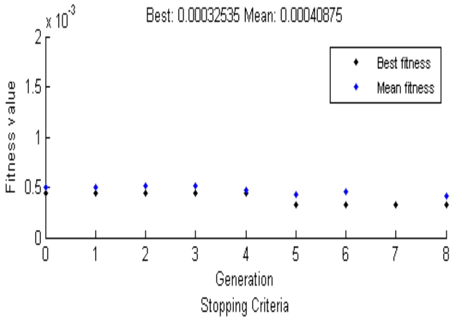

Figure 3: comparison between block selection and region selection

Best fitness is for block selection and mean fitness is for feature region selection [1].

IV. CONCLUSION

In this paper, a method based on DCT domain using MDKP solving procedure is developed to select image blocks for robust digital image watermarking under the constraint of preserving image quality. The robustness of the watermark is significantly improved and image quality after watermarking is still preserved. The development of a MDKP techniques leads to numerous perspectives. The next step of the work can be JPEG watermarking. The techniques proposed in this paper can help validate claims of ownership that required for intellectual property law enforcement.

REFERENCES

[1] Jen-Sheng Tsai, Win-bin Huang and Yau-Hwang Kuo, "On the Selection of optimal Feature Region Set for Robust Digital Image Watermarking", *IEEE Transactions on Image Processing, Vol.20,No.3,March 2011.*

[2] Patrick Bas, Jean-Marc Chassery, and Benoit Macq, "Geometrically Invariant Watermar king Using Feature Points", *IEEE Transactions on Image Processing, Vol.11,No.9,Sepetember 2002.*

[3] Munesh Chandra, Shika Pandey, and Rama Chaudary, "Digital Watermarking Technique for Protecting Digital Images", *IEEE 2010.*

[4] Inegar J. Cox , Joe Kilian, F.Thomson Leigthon and Talal Shamoon , "Secure Spread Spectrum Watermarking for multimedia", *IEEE Transactions on Image Processing, Vol.6,No.12,December 1997.*

[5] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", *IEEE Transactions on Image Processing, Vol.51, No.4, April 2003.*

[6] Jin S. Seo and Chang D.Yoo, "Image Watermarking Based on Invariant Regions of Scale-Space Representation", *IEEE Transactions on Image Processing, Vol.54, No.4, April 2006.*

[7] E.Koch , J.Rindfrey and J.Zhao, "Copyright Protection of Multimedia Data", in proceedings International Conference Digital Media and Electronic Publishing,1994.

[8] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems*. Berlin: Springer,2004.

[9] Jen-Sheng Tsai, Win-bin Huang, Chao-Leigh Chen, Yau-Hwang Kuo "A Feature-Based Digital Image Watermarking for Copyright Protection and Content Authentication" *IEEE, 2007*

AUTHORS

First Author – Mr A. Chandra, Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College, A.Rangampet, Tirupathi, India

Second Author – Ms. T. Kavitha, Mr A. Chandra, Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College, A.Rangampet, Tirupathi, India

Mr. A.Chandra was born in Katherapalli, Chittoor(Dt), A.P.,India. He received his B.Tech degree in Computer Science and Engineering in ersity, Hyderabad. He had his NTUA, Anantapur. His research ocessing, computer networks and ently he is working as Assistant professor in the Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College, A.Rangampet, Tirupati.

Ms. T.Kavitha was born in Chittoor, A.P, India. She received her B.Tech degree in Computer Science and Engineering in sity, Hyderabad. She received her Acharya Nagarjuna University, interests are computer networks Presently She is working as Assistant professor in the Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College, A.Rangampet, Tirupati.