Robust Watermark Extraction Algorithm for Geometrical Compression and Rotational Attacks

Dr. Kesavan Gopal
School of Electronics & Electrical Engineering
Lovely Professional University, Punjab, India
Kesavan.24346@lpu.co.in

Abstract. The main requirement of any watermark extraction algorithm is to withstand the geometrical compression and rotational attacks. Designing of such an algorithm has become prime important with the necessity to extract the watermark from the severest attacks. A new watermark extraction algorithm using color pixel comparison is proposed in this paper. Many watermarking algorithm rely on the ability of extraction procedure which retrieves watermark from the watermarked material, and also how much the quality of extraction algorithm extracts when the watermarked image or video undergoes severe attacks [3]. With the existing watermarking algorithms will not extract the watermark to a reasonable or viewable range of the watermark embedded in the image or video after severe attacks [1][6]. Using a new watermark extraction algorithm, which compares the attacked image with the original watermarked image, which in turn compared with the original image, we are supposed to extract the watermark under worst attacked condition. By using this procedure watermark supposed to be reconstructed will have distortion even less than 10% of the original watermark. The capability of the new idea withstands almost all type of attacks including, highly rotation, highly downscaling, largest compression, cropping, ambiguity, noise addition, pixel deletion with the existing algorithms will not extract such a quality of watermark, will be useful for extracting watermark from any type of embedded images.

Keywords: Robust Watermark Extraction Algorithm, Geometrical Compression, Sub-Decimal Rotational Attacks

1 Introduction

Until recently, a particular watermark embedding and extracting algorithms are suitable only to concentrate of particular application and its requirements, and the algorithms so designed is required to withstand only for few typical attacks which is related to that application [4]. For example in LSB modification [4] done in spatial domain will not with stand huge down scaling, huge JPEG compression, while it is providing visual perceptual. Suppose all the LSB bits changed to either '0' or '1' renders the watermark un-extractable. Watermark embedded in this method are highly vulnerable to even simple attacks. In Correlation based method [4] the gain factor used to improve the robustness should always degrades the watermarked image to a certain level, the main problem of this approach is the extraction of the watermark using threshold, note that threshold values may be highly changed due to various attacks, which renders the watermark invisible. In Discrete Cosine Transform (DCT) [4] based approaches even though it is sustaining attacks like low pass/high pass filtering or median filtering of the image, the extracted watermark from the severely attacked image is not in a position to claim the ownership of the image, due to excessive degradation of the watermark after severe attacks. In DFT (FFT) based approaches [4] which are said to be highly rotation invariant, will not give superior quality watermark when the watermarked image is subject to severe attacks (like 0.1 degree rotated images), in such conditions, extracting the high quality watermark embedded in the host image is impossible.

2 The New Extraction Algorithm

The algorithm described here is non-blind, since it uses both the original image and watermarked image along with the attacked image.

Algorithm:

Step 1: Create a dummy array of the size equal to the size of the watermarked array (for example here 256 x 256).

Step 2: Read the pixel color value (RGB) of attacked image in row wise (like (1,1), (1,2). so on).

Step 3: After reading pixel (1,1) of attacked image look for the same color pixel exist in the watermarked image (search all the pixel of the watermarked image), if pixel found, fill up the dummy array with the same pixel color at the same co ordinates as that of the watermarked image.

Step 4: Read the next pixel color of attacked image (here say (1,2)), repeat the step 2 & 3 till all color pixels of the attacked image has been read off.

Step 5: If the color values read from the attacked image is not found in any locations of the watermarked image, leave the read color value, go for the next pixel.

Step 6: At the end of reading all color pixels from the attacked image, if the dummy array is not completely filled, then fill them either using black or white color pixel value or with the same color as that of the attacked image.

Step 7: Use this dummy array for extracting the watermark in comparison with that of the original image.

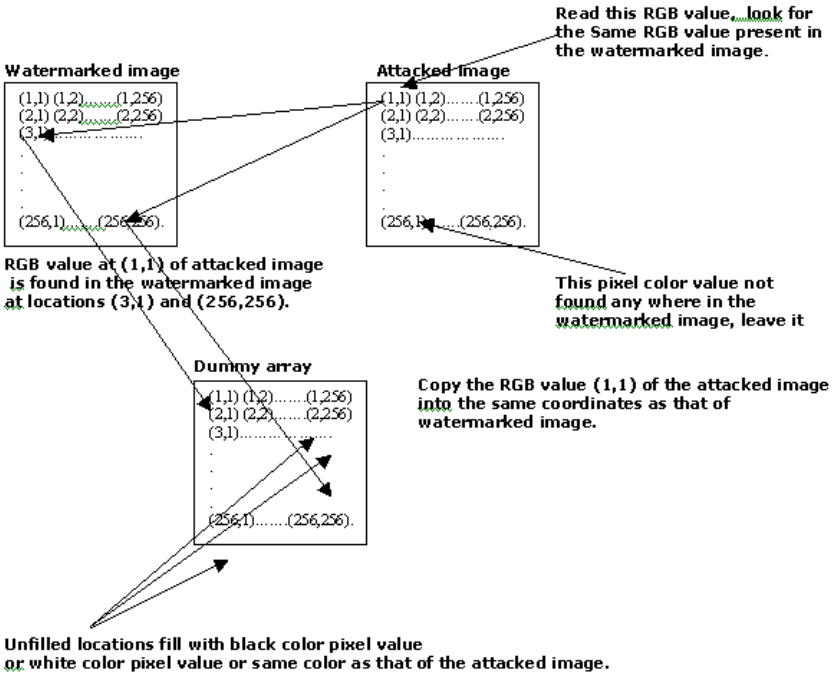

Fig. 1. Illustration of New watermark Extraction Algorithm

3 Testing of Algorithm

The new algorithm presented here is tested by using the embedding and extracting procedure presented in [1][2]. After watermarking an image as prescribed in the paper [1] attack the watermarked image using photo shop tools

Fig. 2. Original image

Fig. 3. Watermarked image

Fig. 4. Watermark

Fig. 5. Watermark piece

3.1 Extraction from rotated image

Subject the watermarked image for various angles of rotation even in steps of 0.1 degree using adobe photo shop. Use the new extraction algorithm to fill the dummy array. Use this dummy array for the extraction procedure presented in [1]. The test results shown below indicate that the new algorithm is extremely suitable for rotational attacks. The standard deviation of the watermark extracted is just less than 10 % distortion at any fractional degree of rotation. Even the RST invariant algorithms prescribed earlier may not suitable for fractional degree of rotation, what this algorithm does. The 225.5 deg rotated image and the extracted watermark piece are shown in figure 6 & 7 respectively [5][7][8].

Fig. 6. 225.5 right rotated image

Fig. 7. Extracted watermark piece

3.2 Extraction from JPEG Compressed image

Another worst attack against the watermarked image is the JPEG compression. Using adobe Photoshop the watermarked image is compressed (with compression ratio of greater than 90 %) still we are able to extract the watermark embedded in the host image using the new extraction algorithm, even most of the recent algorithms will not extract the embedded data after a huge amount of compression. The JPEG compressed image (CR= 90%) and the Extracted watermark piece are shown in figure 8 & 9 respectively.

Fig. 8. 90 % Compressed image

Fig. 9. Extracted watermark piece (Camera man)

3.3 Extraction from Down Scaled image

The third worst attack against the watermarked image is the downscaling, beyond a particular range. Even though most of the present day algorithms work good for up scaling without loss of embedded data, but will not do so for down scaling. The watermarked image scaled down to 50 X 50, and the extracted watermark using this new algorithm is shown in figure 10 & 11.

Fig 10. 50 x 50 Down scaled image

Fig. 11. Extracted watermark piece

3.4 Extraction from the Translation of pixels

The fourth attack over the watermarked image is the translation of pixels. The watermark extracted from the pixel-translated image is shown in figure 12.

Fig. 12. Extracted watermark piece from pixel translated image

3.5 Extraction from ambiguity attacks

The worst kind of attack is re-Watermarking of the watermarked image, which leads to a false claim of the ownership of the image. The new algorithm extracts absolutely the first watermark from the re watermarked image with which the most of the algorithms fails. The Lena (color image) first watermarked by using Cameraman followed by Lena gray image is shown in fig 13 and the extracted piece is also shown in fig 14.

Fig. 13. Watermarked first with Camera man then with lena

Fig. 14. Extracted watermark piece from Re-watermarked image

3.6 Extraction from non-worst attacks

The other forms of attacks, which are not worst in terms of image processing, are also tested and the test results are presented here.

Fig. 15. 800 x 800 up scaled image

Fig.16. Extracted watermark piece

Fig. 17. Guassian blurred image

Fig. 18. Extracted watermark piece

Fig. 19. Guassian noise (0.59) added

Fig. 20. Extracted piece of watermark

Fig. 21. Sharpened image

Fig. 22. Extracted watermark piece

Fig. 23. Sharpened Edges

Fig. 24. Extracted watermark piece

Fig. 25. Cropped image

Fig. 26. Extracted watermark piece

4 C-source code for pixel comparison

```
/*dummy[][] dummy array to be filled

/* final attacked image

/*final1 watermarked image

l=0;

  for(i=0;i<M;i++)

    for(j=0;j<N;j++)

{

 dummy[i+1][j+1].r =255; dummy[i+1][j+1].g =255;

 dummy[i+1][j+1].b =255;

}

  for(i=0;i<M;i++)

   for(j=0;j<N;j++)

{  l=0;

 for(k1=0;k1<M;k1++)

 for(k2=0;k2<N;k2++)

{

   if((Final1[i+1][j+1].r ==Final[k1+1][k2+1].r) &&

 // attacked, watermrked.

     (Final1[i+1][j+1].g ==Final[k1+1][k2+1].g) &&

     (Final1[i+1][j+1].b ==Final[k1+1][k2+1].b))

   {

 dummy[k1+1][k2+1].r=Final1[i+1][j+1].r;

 dummy[k1+1][k2+1].g=Final1[i+1][j+1].g;

 dummy[k1+1][k2+1].b=Final1[i+1][j+1].b;

   }

}

if((dummy[i+1][j+1].r == 255) &&  (dummy[i+1][j+1].g ==255) &&   (dummy[i+1][j+1].b
==255))

    {

 dummy[i+1][j+1].r=Final1[i+1][j+1].r;

 dummy[i+1][j+1].g=Final1[i+1][j+1].g;
```

```
    dummy[i+1][j+1].b=Final1[i+1][j+1].b;

     }

  }
```

5 Advantage

The advantage of using this type of algorithm is that it extracts the watermark embedded in the host images even after the worst attacks which may not be the case as compared with the algorithm presented in [1] for DWT's and in [4] for DCT's.

6 Disadvantage

With the above the mentioned advantages, the disadvantage of the algorithm is that dissimilar images of at least 50% same color pixel values still extracts the watermark, from that image which is not actually watermarked or not our own, and the occurrence of such a situation is rare and hopefully the owner knows, by viewing an image which is his own or not. If the owner realizes that the image is not his own, he never tries to extract the watermark from that image. This helps to overcome the disadvantage of this new extraction algorithm.

7 Conclusion

Thus the techniques presented here can be extended to any size of image, algorithm highly suitable for any watermarking algorithm with excellent performance. The scheme can be extended by making use of information from the video, optimizes the complexity of any type of extraction algorithm, tested this algorithm for various types of Embedding/Extraction techniques, and suppose to be implemented in Hardware (FPGA boards).

References

1. Chan Pik Wah, "Multimedia Security- Digital video watermarking, Term paper (Fall 2002) pp.30-45.

2. Pik Wah Chan and Michael R.Lyu, " A DWT-based Digital video watermarking scheme with error correcting code".

3. Nicholas D.Beser, Thomas E.Duerr, Gregory P. Staisionas, "Authentication of Digital Video Evidence".

4. http://www.watermarkingworld.org.

5. J.G.Proakis," Digital Signal processing" Mcgraw Hill, 1998.

6. Iwan Setyawan, Information and Communication theory group," Attacks on Watermarking Systems", Deltt university of Technology.

7. Xiamu Niu, Martia Schmucker, Christoph Busch, "Video watermarking Resisting to Rotation Scaling and Translation", Fraunhofer institute for computer Graphics (IGD), Germany.

8. M.Kutter,"Watermarking Resisting to Translation Rotation and Scaling," Proceedings of SPIE , November 1998.