Piecewise Watermarking by clustering using similarity measure in Images

Mrs.S.Kavitha[#1], Dr.N.Subhash Chandra [*2]

[#] *Research Scholar ,JNTUH,Hyd*

**Director of Academics, Holy Mary Institute of Technology and Science, Hyd*

Abstract— *With the growth of sharing the personal pictures in social media publically has urged the researchers to protect the ownership rights on the images from morphing, Copying, Misusing etc., Techniques that are already in use are prone to various attacks like geometric attacks, removal attack, Cryptographic attack, protocol attack etc., In this paper a better technique is proposed that can successfully prove the ownership rights on the images and can sustain many types of attacks .*

Keywords— *Watermarking, Digital Rights Management, Clustering.*

I. INTRODUCTION

Now a days posting the personal pictures in the Social Media publically has become very common among the people who are more acquainted with social networking sites. This raised an issue whether the images that are shared are tampered, morphed, copied or misused. In order to claim that it has not been modified, many watermarking techniques were developed. Most of the techniques are prone to various types of attacks like removal attacks, geometric attacks, cryptographic attacks, and protocol attacks In removal attack watermark information is removed from the watermarked data image without any in detail knowledge about the technique used to embed the watermark. Geometric attacks [1] do not remove the watermark try to find the algorithm used in embedding watermark. Cryptographic attacks aim to find the algorithm used in embedding watermark or try to change the embedded watermark. Protocol attack [5] in this type of attack attacker changes the watermarked image and claims to be the owner of the image. In detail attacking techniques can be found in [1 , 6].

In this paper a different technique which uses multiple watermarks on different areas of the image which are clustered using clustering algorithm based on similarity measure has been proposed which happens to be a method that can prove ownership rights on the digital image even after different attacks performed on it.

Watermarking algorithms should satisfy the following properties

a) Robustness: The algorithm used in embedding watermarking should have the ability to withstand non-malicious distortions to sustain removal attack etc.,

b) Data payload: Encoded message size of the watermark embedded in the image. The algorithm used in encoding should be unambiguous.

c) Capacity: It is the amount of watermarked information in an image. Capacity should not affect the actual quality of the image.

d) Imperceptibility: If any kind of watermarking technique is used like blind watermark etc., then imperceptibility refers to the characteristic of hiding a watermark such that original quality of the image is not lost.

e) Security: It is the ability of the watermark to resist against malicious attacks.

.

II. EXISTING SYSTEM

In Existing system Jen-sheng Tsai [7] proposed a image watermarking technique based on feature region set selection but the algorithm used cannot sustain Geometric attacks. Xiaolong Li [8] proposed a watermarking technique based on selected pixel but it is also prone to geometric attack. Ehsan Nezhadarya, proposed a technique based on multi-scale gradient which cannot sustain many types of attacks. Many more algorithms were proposed but they are prone to various attacks, due to which proving ownership rights on the image has become difficult in this digital world.

III.PROPOSED SYSTEM

In the proposed system image is formed into different classes based on the similarity measure between different pixels, here we don't consider any particular regions. The pixel gray level is considered for mapping the similarity. If the similarity matches they are considered as on class. In each class different watermark is embedded so that any kind of attack occurs other watermark is used as ownership detection. As embedding multiple watermarks in single image makes the system clumsy. Hence, number of different watermarks are restricted to maximum of there i.e., the number of classes in cluster is restricted to three. After embedding watermark hashing is performed on each class separately and encrypted to ensure integrity and security against modification of the image.

A. ALGORITHM FOR CLUSTURING

Step 1: The original RGB image is converted to gray scale image and represented as rows X cols as follows

TABLE I
GRAY SCALE REPRESENTATION OF THE IMAGE

X / Y	Col 1	Col 2	Col 3	Col 4	Col 5	Col 6	Col 7	Col 8
Row 1	37	31	32	26	26	17	21	22
Row 2	18	26	36	56	56	33	22	28
Row 3	23	45	57	78	76	39	18	21
Row 4	21	62	84	77	77	58	46	34
Row 5	25	50	77	72	74	71	71	71

Similarity between pixel at col 1 and col 2 is defined as

SIM (Col $_i$, Col $_j$)= $\sum_{k=0}^{n}$ (Col $_{k,i}$)(Col $_{k,j}$)

'k' is summed across the set of all items. The result is n X n matrix, where n is number of columns. Apply the similarity formula by using following algorithm

Step a) Read the original image

```
c1=imread('flow.jpg');
```

Step b) Convert into gray scale image

```
c=rgb2gray(c1);
```

Step c)Select a region in the image randomly

```
x=c(201:205,201:208);
```

Step d) Using Similarity measure construct similarity matrix

```
for i=1:8
  for j=1:8
    b(i,j)=uint32(0);
    for k=1:5
      if i==j
      b(i,j)=0;
      else
      b(i,j)=uint32(b(i,j))+uint32(x(k,i))*uint32(x(k,j));
       end
      end
  end
end
```

Step 2 : Convert the above matrix into binary matrix by selecting a threshold. Apply the following algorithm to convert it to binary matrix where y is the binary matrix.

```
for i=1:8
    for j=1:8
        y(i,j)=0;
        if(b(i,j)>7000)
            y(i,j)=1;
        end
    end
end
```

Step 3: Perform the cluster using following algorithm

```
for t=1:8
    rc(t)=0;
end
cx=0;
 p=0;
for i=1:8
       if rc(i)==0
         p=p+1;
         cx=cx+1;
         class(cx,p)=i;
         rc(i)=1;
    end
    li=i+1;
    for j=li:8
        if rc(j)==0
            if y(i,j)==1
                p=p+1;
             class(cx,p)=j;
             rc(j)=1;
            end
        end
            end
 end
for i=1:cx
    for j=1:8
        if class(i,j)~=0
           class(i,j);
        end
    end
end
```

The resultant classes are

Class(1)={pixel $_{1,1}$, pixel $_{14}$, pixel $_{1,5}$, }
Class(2)={pixel $_{1,2}$, pixel $_{1,3}$, pixel $_{16}$,pixel $_{1,8}$, }
Class(3)={pixel $_{1,7}$}

Step 4: Calculate the centroid of each class by taking the average of the members in each class respectively

```
Class(1)=  [30,43,59,58,57];
Class(2)=  [25,49,24, 68];
 Class(3)= [57]
Cenx=class(1);
Ceny=class(2);
Cenz=class(3);
```

Step 5: Now Assign each pixel in the image to respective class by calculating the similarity of the pixel with the class as

SIM (pixel $_{i,,}$, class $_j$)= $\sum_{k=0}^{n}$ (pixel $_{k,i}$)(pixel $_{k,j}$)

```
for i=1:320
  for j=1:240
    r1(i,j)=0;
    r2(i,j)=0;
    r3(i,j)=0;
     calc1=uint32(0);
     calc2=uint32(0);
     calc3=uint32(0);
    for k=1:5
calc1=uint32(calc1)+uint32(uint32(cenx(k))*uint32(c(k,j)));
calc2=uint32(calc2)+uint32(uint32(ceny(k))*uint32(c(k,j)));
calc3=uint32(calc3)+uint32(uint32(cenz(k))*uint32(c(k,j)));
```

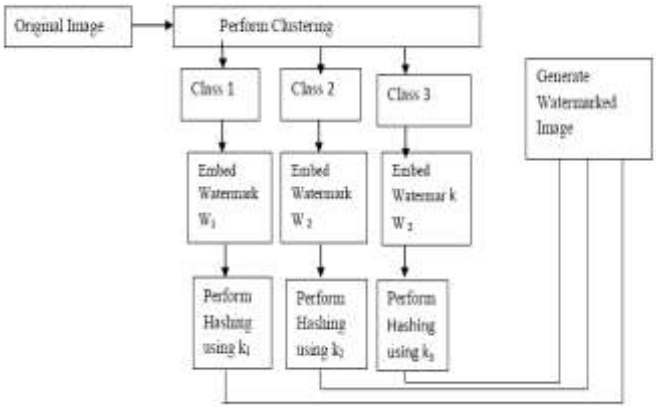
```
        end
          if(calc1>calc3)
             if(calc1>calc2)
             r1(i,j)=c(i,j);
             else
             r2(i,j)=c(i,j);
             end
          else
             r3(i,j)=c(i,j);
          end
          end
end

for i=1:320
   for j=1:240
      s1=r1(i,j);
      s2=r2(i,j);
      s3=r3(i,j);
      s=s1+s2+s3;
      h(i,j)=s;

   end
end
```

B. ALGORITHM FOR EMBEDDING WATERMARK

Step 1: Select three watermark and insert the watermark using normal embedding process.

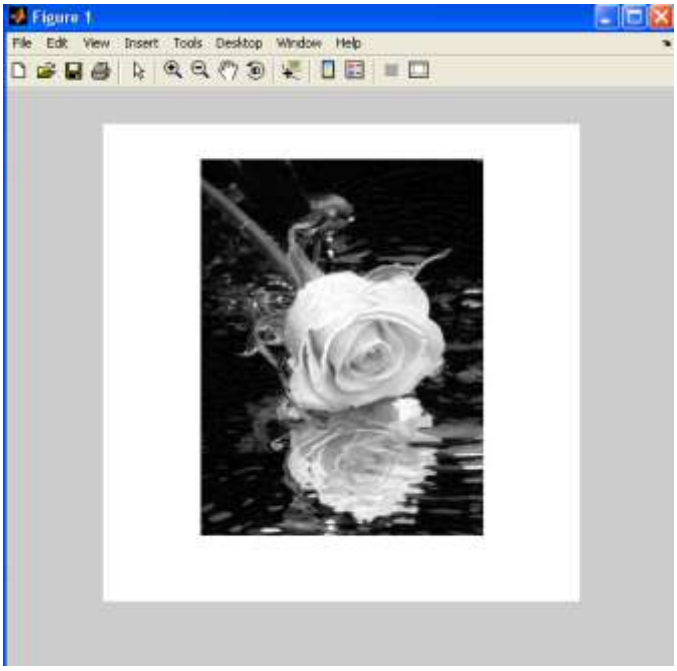


Step 2: Perform hashing on the each class using a different key respectively

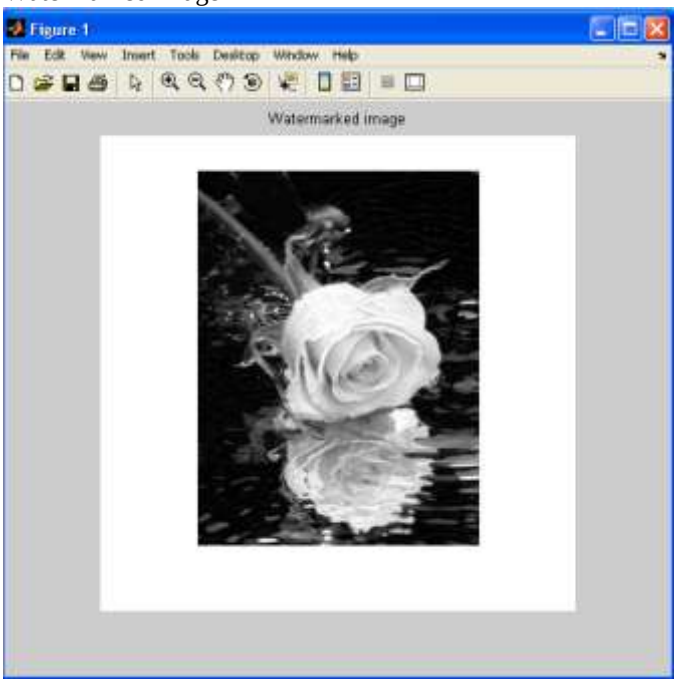
Step3: Generate watermarked image by performing image addition on three different clusters separately.

Experiment and Results:

Original image



Watermarked image



IV. CONCLUSIONS

In this paper a new technique of embedding watermark in an image has been proposed. The Algorithm used for clustering is used to ensures the categorization of parts in the image which is not done through normal region extraction algorithms. As it uses three different watermarks if any part of the image is tampered other regions can be used for copy right

protection. The Hashing algorithm used ensured integrity of the image. The techniques protects the image from different attacks based on geometric attacks.

REFERENCES

[1] S. Voloshynovskiy, S. Pereira, V. Iquise and T. Pun, "Attack modelling: Towards a second generation watermarking benchmark," Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.

[2] J. K. Su, J.J. Eggers and B. Girod, "Analysis of digital watermarks subjected to optimum linear filtering and additive noise," Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.

[3] S. Voloshynovskiy, A. Herrigel, N. B. and T. Pun, "A stochastic approach to content adaptive digital image watermarking," In *International Workshop on Information Hiding*, Vol. **LNCS 1768** of Lecture Notes in Computer Science, pp. 212-236, Springer Verlag, Dresden, Germany, 29 September -1 October 1999.

[4] P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," submitted to IEEE Trans. Inform. Theory.

[5] S. Craver, N. Memon, B. Yeo, and M. Young, "On the invertibility of invisible watermarking techniques," Proc. Of the IEEE Int. Conf. On Image Processing 1997, Vol. 1, p. 540-543.

[6] F. Hartung, J.K. Su, and B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counter-Attacks,"

[7] 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

[8] Xiaolong Li, Bin Yang, and Tieyong Zeng Efficient "ReversibleWatermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 12, DECEMBER 2011

[9] Ehsan Nezhadarya, Z. Jane Wang ,Rabab Kreidieh Ward," Robust Image Watermarking Based on Multiscale Gradient Direction Quantization", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 4, DECEMBER 2011