Robust Image Watermarking Based on Histogram Shape and Butterworth Filtering

Kiran[1] Dr. Kanwal Garg[2] Girdhar Gopal[3]
[1]Research Scholar (M. Tech) [2,3]Assistant Professor
[1,2,3]Department of Computer Science and Applications
[1,2,3]Kurukshetra University, Kurukshetra

Abstract— In the image watermarking community, developing a robust watermarking method has attracted increasing attention in recent years. In this paper, robust image watermark algorithm is proposed which is based on histogram shape that resists against geometric attack and signal processing attack by using invariance property of histogram to scaling and statistically independent to the position of pixels in the image. In this method, watermark is embedded by shifting pixels within group by maintaining histogram shape. At watermark detection site, watermark is detected by calculating relationship between bins of group. Watermark scheme is blind in nature.

Key words: Geometric Attack, Histogram Shape, PSNR, Quality

I. INTRODUCTION

In today's era, technology has made the transmission of digital media objects as a walk in the park and digital media can be easily reproduced and manipulated, so copyright protection of digital media content is necessary, Digital watermarking is solution to this problem. Digital watermarking is a technique in which pattern of bits is embedded into original image or cover image or host signal with the help of algorithm called embedding algorithm and resultant is called watermarked image or stego image which is further attacked either intentionally or unintentionally that results in distorted image . At the receiver side, watermark is extracted with the help of extraction algorithm and get the extracted image [1]. In this paper, emphasis is done on image watermarking Digital watermarking possess many characteristics. These are described as follow:

- Imperceptibility: Change made to digital content is imperceptible. It do not loose visual quality.
- Robustness: Digital content is withstand against various attacks like rotation, scaling, translation, compression, noise, shearing etc.
- Capacity: Amount of data is embedding in digital content. It is inversely related to robustness and imperceptibility.
- Security: capability of watermark is to withstand against malicious attack.

Attack can be classified into geometric attack and signal processing attack.

Geometric can be further classified into invertible attack and non-invertible attack. Invertible attack includes affine transformation such as rotation, scaling, translation and random bending attacks and non-invertible attack includes cropping [2]. A geometric attack induces two types of distortion in image. One is shifting of pixel in image and other is modification of value of pixel of image, call it as interpolation errors. Interpolation errors include edge halos, blurring and aliasing [3]

In this paper, interpolation errors only distort the value of pixel, does not do the blurring, aliasing, and edge halos as the histogram is independent of the pixels position.

In regards to the image watermarking, the interpolation errors under geometric attacks are limited because the attacked image should keep an acceptable level of visual quality. Due to this, the histogram shape of the low-frequency component of an image has good resistance to geometric attacks. Geometric attacks are more challenging than signal processing attack as geometric attacks produces synchronization errors between the embedder and extractor because it can change the location of pixels and the physical position of watermark. Due to this, the watermark is still present, but the detector is no longer able to extract it [2]. Whereas the content-preserving image processing operations such as addition of noises, common compression and filtering operations reduces watermark energy.

II. RELATED WORK

Lin et.al proposed an algorithm in which a 1-dimension watermark signal derived from the image was proposed to resist rotation, scaling and translation (RST) distortion, but the implementation is a very simple example so the improvement is also needed [4]. Kang et.al presented an image watermarking algorithm that uses combination of DWT–DFT (discrete wavelet transform-discrete Fourier transform)is robust against both affine transformation and JPEG compression, however, the robustness of the informative watermark against median filtering and random bending needs to be improved [5].Lu.et.al derived a hash-based image watermarking algorithm that was composed of mesh generation and hash-based content-dependent watermark. The watermark can be detected without knowledge of original images by sharing the exploited private key in the detector. In addition to the image watermarking there was other watermark form and content [6]. Xiang et al. exploited the statistical property of histogram shape, which is invariant to pixel position shifting and insensitive to cropping. The mean concept is used in the Gaussian filtered low-frequency components of images to resist geometric attacks [2]. In Xuansen et.al [7], watermark is embedded into groups but group consist of three bins and used the statistical invariant property of histogram shape. In,Wang et.al. Binary watermark sequence is embedded based on histogram based and the distances between adjacent elements of histogram are calculated [8].

In this paper, Butterworth low pass filter is used to extract the low frequency component of image then embeds the watermark into this by maintaining histogram shape property, which is independent to pixel position and robust against geometric attacks. It is applied to all images and provides higher robustness because the embedding range selection step is entirely based on the histogram shape.

III. HISTOGRAM

In Statistics, Histogram is a graphical representation showing distribution of data. A histogram has two axis, the x axis and the y axis.

– The x axis contains data whose frequency you have to count.
– The y axis contains frequency of that data.

x contains data set [1 2 3 1 5 0 1 4 3 1 2 4 0 3 5 6] and Fig.1. Shows histogram of data set x

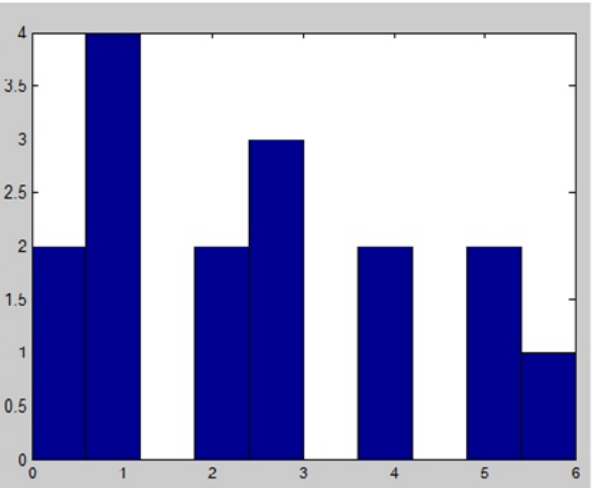

Fig. 1: Histogram of data

In Digital image processing, Histogram is a simple and effective tool to represent the distribution of pixels of image .The Histogram of image is a plot of the number of occurrences of gray levels in the image against the gray level values. It provides a convenient summary of intensities in an image, but unable to convey any information regarding spatial relationships between pixels [9]. In other way, it is a type of histogram that acts as a graphical representation of the intensity value in a digital image.

Histogram is independent of pixel position, that's why this property is used in this paper to maintain robustness against geometric attack like rotation, scaling, translation. Robustness against geometric attack can attain by implementing an invariant property histogram shape (ratio of population of bins). Image histogram is a statistical expression.

The histogram of a digital image I with gray levels in the range [0, L-1] is a discrete function

$$H(k) = \{h(k) \mid k=0, 1 \ldots\ldots L-1\} \quad (1)$$

h(k) denotes the number of pixels corresponding to k gray level of the digital image I and

$$M*N = \sum_{k=0}^{255} h(k) \quad (2)$$

Where M and N are number of rows and number of columns of image I respectively. Value of I(x, y) represents intensity value (gray level value) at position (x, y). In 8 bit gray scale image, 8 bits represents bit depth. 256 gray level are there i.e. from 0 to 255 means each pixel of gray scale image possess intensities value within range of 0 to 255. The relation between the number of the bins Land the bin width M is [2] depicted as

$$L = 2^p / M \text{ if } Mod(2^p / M) = 0$$
$$\lfloor 2^p / M + 1 \rfloor \text{ otherwise} \quad (3)$$

Where h(k) includes those pixels between (i-1). Mand i.M-1, p is bit depth.

IV. HISTOGRAM WATERMARK EMBEDDING ALGORITHM

1) Step 1: Input image

After reading the image file, get the data matrix of original image I(i, j), i = 1: M, j = 1: N, Mand N respectively stands for the row and column of host image.

2) Step 2: Butterworth filtering

Apply Butterworth low pass filter to extract low frequency component of image (I_{low}).

3) Step 3: Histogram Extraction

Construct the histogram of low frequency component of image

$$H_{low}(k) = h_{low}(k), k=0,1\ldots\ldots L-1$$

Denotes number of pixels of intensity value k

4) Step 4: Watermark Embedding Range Selection

Select the groups whose number of pixels is greater than T_a. Denote these numbers of groups as S and choose L groups with most number of pixels out of S for watermark embedding.

5) Step 5: Watermark Embedding:

The watermark W is a key-based PN sequence whose length L is embedded by maintaining histogram shape (ratio between numbers of pixels of two bins). It is represented as

$W = \{ w(i) \mid i = 0, 1, \ldots, L\}$

$b1/b2 >= T_c$ if $w(i)=1$

$b2/b1 >= T_c$ if $w(i)=0$ (4)

Watermark embedding is done in the low frequency component of image and get the low frequency component of watermarked image (I^w_{low}).

6) Step 6: Watermarked Image

Obtain the watermarked image by combining high frequency component of image (I_{high}) and low frequency component of watermark image (I^w_{low}).

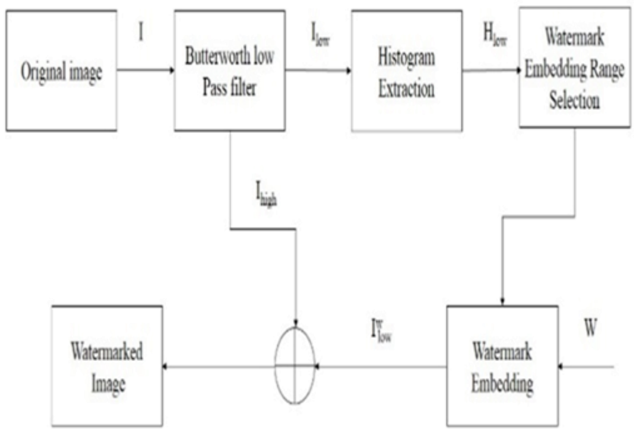

Fig. 2: Block Diagram of Watermark Embedding Process

A. *Butterworth Low Pass Filter:*

Butterworth low pass filter is lowpass filter in frequency domain which is radially symmetric. It basically smooth out the image, blur the edges and reduces the noise. Frequency filters process an image in the frequency domain. The image is first, Fourier transformed, then multiplied with the filter function, and then transformed back to the spatial domain.

Robustness to common signal processing attacks can be achieved by embedding watermarks into the low-frequency component of an image [10]. Thus, we first Pre-process the host gray scale image I by a 2-D Butterworth low-pass filter.

$$H(u, v) = 1 / [1 + D(u, v) / Do]^{(2*n)} \quad (5)$$

Where D(u, v) is the distance from any point (u, v) to the center of the Fourier transform, Do is the distance of the cutoff frequency, and n is the order. Do control the radius of the filter and n controls how steep or sharp the transition is at the edges of the filter [11].

The lowpass filtering operation can be represented as the multiplication of the image in transform domain and Butterworth low pass filter.

$$I_{low}(u,v)=I(u,v)* H(u, v) \quad (6)$$

Where I(u ,v) represents image in transform domain, H(u, v) is Butterworth filter, I_{low} (u, v) is low frequency component of image in transform domain.

B. Embedding Range Selection:

In this phase, location of adding watermark is find out. For this firstly the host image I is passed through a Butterworth low pass filter to extract its low-frequency component I_{low}. Then the histogram H_{low} of I_{low} will be extracted, which can be expressed as

$$H_{low} = \{h_{low}(k) \mid k=0,1,\dots,255\} \quad (7)$$

Where $h_{low(k)}$ represents the number of pixels in I_{low} whose pixel values are k. Different from the method in [2], we first combine the neighboring two gray levels in H_{low} as one bin. The bin vector C can be represented as

$$C = \{c(k)|k= 0, 1, ..,\lfloor 255/2\rfloor\} \quad (8)$$

Where⌊·⌋is the floor function. The combining process can be expressed

$$c(k)= h_{low}(2.k)+h_{low}(2.i+1) \quad (9)$$

Then group is formed by combining adjacent two bin. So, group vector is given as

$$D = \{d(k)|k = 0, 1, \dots, \lfloor 255/4\rfloor \quad (10)$$

D can be expressed in terms of bins [12] as

$$d(k) = c(2 \cdot k) + c(2 \cdot k+ 1). \quad (11)$$

Number of pixels in the kth group is denoted as N_{dk}. Range for watermark embedding is based on number of pixels in group and T_a. T_a is predefined threshold that controls robustness, quality and embedding rate. Scan all groups of D vector, choose the groups that satisfy this certain criteria . If N_{dk} is greater than a pre-defined threshold T_a, then the kth group will be selected for watermark embedding, otherwise leave the kth group as it is not selected for watermark embedding. In this way, candidatures are choosed for watermarking. Selected groups are Sand the length of the watermark as L, where L≤ S. Choose L groups with most number of pixels out of S for watermark embedding and leave the rest groups. So, watermark embedding range selection is completed by accompanying this step.

C. Watermark Embedding:

After the embedding range is selected, watermark embedding is done by shifting number of pixels within group from one bin to another if certain criteria are not fulfilled. To achieve this, firstly ratio of number of pixel of consecutive bins of that group is calculated. For the ith selected group, there are two bins in it, bin1 and bin2 (10). Denote the numbers of pixels in bin1 and bin2 as b1 and b2 respectively. The watermark W is a key-based PN sequence which is represented as

$$W= \{w(i)|i= 0, 1, \dots, L\} \quad (12)$$

Choosing of PN sequence is that, it offered a good synchronization capability due to its correlation property. Regeneration capability at detector side is good [7]. The number of watermarking data bits should be less than the number of groups of the histogram as one group accommodate one watermark bit. The private key is shared with the detector during the decision-making for presence of the watermark as used in [11]

The embedding rule for the ith watermark bit is computed as

Watermark embedding bit, w(i) ==1

If b1/b2 >= Tc then no operation is needed Else randomly select N_{w1} pixels and shift the pixels from bin2 to bin1 in such way that intensity value of N_{w1} pixels of bin2 is changed to intensity value ofbin1. By this way, histogram of image corresponding to the bin is changed. By doing this ratio is no longer remained less than Tc. where Tc is a pre-defined threshold balancing the robustness and perceptual quality. In this paper Tc is set to 2.

Watermarking embedding bit w(i)==0

If b2/b1 >= Tc then no operation is needed

Else randomly select N_{w0} pixels and shift the pixels from bin1 to bin2 in such way that intensity value ofN_{w0} pixel of bin1 is changed to intensity value of bin2. By doing this, ratio is no longer remain less than Tc and histogram of image in regards to bin is changed but not to group. N_{w0} and N_{w1} is computed as

- N_{w1}=Tc.b1-b2/1+Tc
- N_{w0}=Tc.b2-b1/1+Tc

In this way, all L bits of watermark are inserted into low frequency component of image and low-frequency component of the watermarked image(I^{w}_{low}) is attained .Each selected group carry one watermark bit. I^{w}_{low} and the high-frequency component of I (I_{high}= I-I_{low}) are merged and got the watermarked image.

V. HISTOGRAM WATERMARK EXTRACTION ALGORITHM

1) Step 1: After reading the watermarked image file I` , get a data matrix I`(i, j), i = 1:M, j = 1: N, M and N stand for the row and column of host image.
2) Step 2: Butterworth filtering

Apply Butterworth low pass filter to extract low frequency component of watermarked image (I`$_{low}$)

3) Step 3: Histogram Extraction

H`$_{low}$ (k)=h`$_{low}$ *(k)* ,k=0,1……..L

Denotes number of pixels of intensity value k

Divide the histogram bins as groups, each group consist of two adjacent bins (bin1 and bin2) and their population is b1` and b2` respectively.

4) Step 4: Watermark Embedding Range Selection

Select L groups with most number of pixels as watermarked groups.

5) Step 5: Watermark Detection:

By computing the ratio between b1` and b2` of each group, one inserted bit is extracted in reference to the following equation,

- w`(i) = 1, if b1` / b2` ≥ 1
- w`(i) = 0,otherwise.

The process is repeated until all bits are extracted.

6) Step 6: Watermark Extraction:

Extracted watermark is depicted as

W`= w`(i)| i=0,1,2…….L

All L bits are extracted.

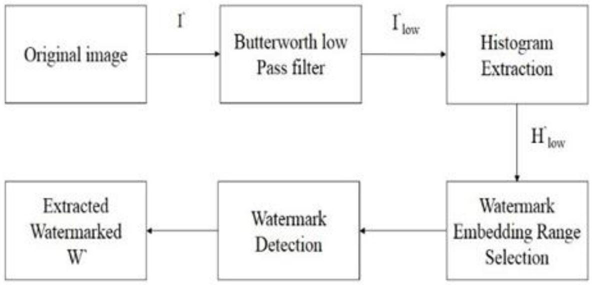

Fig. 3: Block Diagram of Watermarking Extraction Process

VI. CONCLUSION

This paper proposes robust image watermarking scheme by using the property of the histogram shape to be independent of the pixel location, mathematically invariant to the scaling. Embedding of watermark is done in low frequency component of Butterworth low pass filter. Watermark is extracted without knowledge of original image. The proposed algorithm is robust against different geometric attacks rotation, scaling, translation, cropping ,random bending attack and signal processing attacks like additive noise, Gaussian noise, compression etc.

REFERENCES

[1] Kiran and kanwal garg, "Digital watermarking:Potential challenges and Issues," International Journal of Computer Science Engineering and Technology, vol. 5, no. 3, pp. 48-50, 2015.
[2] Shijun Xiang, Hyoung Joong Kim, and Jiwu Huang, "Invariant Image Watermarking Based On Statistical Features in the Low Frequency Domain," IEEE transaction On circuits and system for video technology, vol. 18, no. 6, pp. 777-790, june 2008.
[3] (2008) Colour understanding Digital Image Interpolation. [Online]. http://www.cambridgeincolour.com/tutorials/
[4] Lin, I.j.Cox, and Miller, "Rotation,scale and translation resilient public watermarking for images," IEEE Trans. on Image Processing, vol. 10, no. 5, pp. 767-782, 2001.
[5] X. Kang, J. Huang, Y. Shi, and Y. Lin, "A DWT - DFT Composite Watermarking Schme Robust to both Affine Transform and JPEG compression," IEEE trans. on Circuit and system for video technology, vol. 13, no. 8, pp. 776-786, 2003.
[6] S. Lu, C. Sun, and Chang, "Robust Hash Based Image Watermarking with Resistant to Geometric Distortion and Watermark Estimation attack," in in Proc. SPIE-IS&T Electronics Image SPIE 5681, 2005, pp. 147-163.
[7] Xuansen He, Tao Zhu, and Gaobo Yang, "A geometrical attack resistant image watermarking algorithm based on histogram modification," Springer, pp. 291-306, October 2013.
[8] Shumei Wang and Wenbao Hou, "A Robust Watermarking Algorithm Based On Histogram," in Proc. IWSA, China, 2009, pp. 453-456.
[9] S Jayaraman, S Esakkirajan, and T Veerakumar, Digital Image Processing. New Delhi, India: Tata McGraw Hill, 2009.
[10] Tianrui Zong, Yong Xiang, Iynkaran Natgunnathan, Wanlei Zhou, and Gleb Belikov, "Robust histogram shape based method for image watermarking," IEEE Trans. Circuits and SystemsFor Video Technology.
[11] [Online]. http://www.cs.utah.edu/~croberts/courses/cs7966/project3/
[12] Tianrui Zong, Yong Xiang, and Iynkaran Natgunanathan, "Histrogram Shape Based Robust Image Watermarking Method," IEEE ICC Communication and Information System Security Symposium, pp. 878-883, 2014.
[13] H.Zhang, H.Z.Shu, J.Zhu,H.Q.Zhu G.Coatrieux, and L.M.Luo, "Affine Legendre Moment invariants for image watermark robust to geometric distortions," IEEE Trans. Image Process, vol. 20, no. 8, pp. 2189-2199, 2011.