Copyright for Images with Chaotic Sequence

Prof.P.M.Patil, Mr.Shreyas Shinde, Miss.C.V.Arekar , Miss.N.M.Bhandwalkar
Vidya Pratishthan's College of Engg, Baramati
Pune- 413133

Abstract— ***Now days more people are use photos to record their special activities; and they will share these photos and information to others via internet. But, these photos may be used without permission after they are uploaded to Internet. To coming out from this problem, invisible watermarks into images will be done. Also, an additional for watermarking process embedding watermarks should be apply before an image is up-loaded on internet. But sometimes the numbers of photos are large then the watermarking process will be lengthy to user. Thus we propose a Digital watermarking for copyright on Android platform. By using this system, pre-specified copyright information is automatically embedded into pictures with digital watermark technology before uploading on internet. In addition, original images (i.e., images without watermarks) can be achieved as its original form. .Therefore, this system is very suitable for the protection of the photographs which are used by Android phones to prevent piratical behaviors.***

Index Terms—***Android Platform, Chaos Theory, Copyrights image, Digital Watermarking, Messy watermarking algorithm***

I. Introduction

Now days, lot of people use photos for sharing of special events and actions. These photos are uploading on internet via facebook, whatsApp and many more mediums. But these pictures are use without permission of the owner and misuse them by adding any unwanted data. Also these photos are use for adding another faces or changing the background. The piracies of images are increase day by day. Also there are some national and international photography competitions based on best photos. But sometimes these photos are pirated. So we design a system for android to copyright images. People give preference to use android phones, so we give priority to android and create new application to making copyright lot of images. This application create image with some information which gives the copyright permission to that image. By using this system we can avoid lot of piracy of images.

II. Related WORKs

Android is Linux based operating system which provides security, memory management, process management. The watermarking technique is used to security of massage behind image/video.

There are four techniques present to do watermarking as a)additive b) multiplicative c)quantization-based and d)relationship-based. Hsu and Wu proposed an approach using middle frequency coefficients chosen from one or more 88 DCT blocks to embed watermarks. Quantization operation is taken into account in this approach so that watermarks can survive the JPEG lossy compression.

The messy watermarking algorithm has been suggested for medical image security. It creates the watermark dynamically by using messy scheme which is unique to the images. The generated watermark is going to embed in that image by expanding the differences of the pixel pairs in intra color planes of images. It could exactly locate the tampered region in an image.

Chaos is a kind of theory which is about nonlinear dynamics law control the data stream generated in this theory is disordered, and its similar to random noise. The new binary sequence, which is the binarization of acquired chaotic sequence, has two main functions as.

A. It is used to the encryption of text data information, which can enhance the security of the steganography.

B. It is used to stimulate the binary data stream, which can facilitate the process of various experiments.

By chaos theory, it is easy to test the performance of steganography, and the design has higher security and reliability.

Chaos Equation –

$$Xnew = K . Xold (1 - Xold)$$

The reversible data hiding technique is used to obtain the lossless watermarked image in its original form. Normally at the time of extracting watermark form image the quality of original image is getting down, so the solution to this problem reversible data hiding method was introduced. Reversible data hiding techniques have also been proposed for various fields such as audio, MPEG-2 video, 3-D meshes, visible watermarking], SMVQ-based compressed domain, and the integer-to-integer wavelet domain.

III. Proposed Work

A. Problem Definition

The automatic photograph publishing process proposed in this project involves three major tasks:

1) Watermarking embedding
2) Image resizing, and
3) Image uploading.

These three tasks are integrated appropriately into the automatic photograph publishing process to reduce computational complexity Flow diagram of the proposed Automatic photograph publishing process included in the automatic photograph publishing process are described as follows.

1) Transform the photograph into RGB format.

2) Create the Chose sequence with the help of green channel.
3) Add this sequence in image according to blue and red pixels.
4) Add a digital watermark (i.e., copyright information) to the photograph by Messy algorithm.
5) Upload the watermarked photograph to Internet.

B. Scope of Project

We propose a new application for android system which generate the copyright on the images what we want. This application may run on any android version after 3.2.2. Our application uses two different algorithms to create watermarking and adding the information behind the images for copyright purpose. This application may also convert more than one image to make copyright. This application returns the original image from watermark image with its original quality and tell that what changes have been done in that image.

C. Project Objectives

Copyright is a legal means of protecting an author's work. It is a type of intellectual property that provides exclusive publication, distribution, and usage rights for the author. We create this type of copyright system for images which gives the following:

1) No one use the image editing procedure without permission of author.
2) If any type changes are done in image then it easily capture.
3) We provide watermark for security purpose.
4) The original image should be getting after removing watermark.
5) The quality of image should maintain.

D. Project Constraints

1) This application is based on Android platform so it provides high level of security and increase in the speed of operations.
2) No one can use the image which is with copyright access.
3) Watermark can be done on many images at a time in short time than other system.
4) The original image should be after removing watermark.

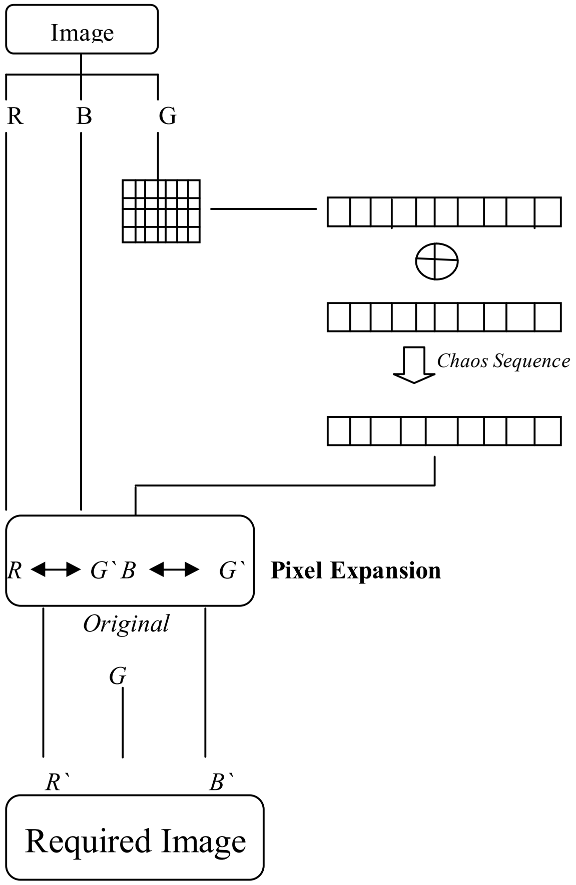
IV. Watermark Generation

A. Separation of Color Plane

We separate here three color plans as R,G,B and take G plane for further procedure. The main reasons of separating plans are

1) Attack Detection
2) Copyright Protection

These two main purposes are achieved by separating plans for the messy algorithm.



B. Apply Chaos sequence for green plane

$$Xnew = K.Xold(1 - Xold)$$

Where X_{new}: New green pixel value
K : constant
X_{old}: Original pixel value

With the help of this equation we generate new green color plane for encryption purpose. By selecting chaos theory, it is easy to test the performance of steganography; also the design may have higher security and reliability.

C. Apply Messy algorithm

Messy algorithm is a dynamical algorithm which changes always. These changes are too much related to initial conditions. These changes are as tremendous growth of anxiety in the initial conditions. Thus, the behavior of messy algorithm appears to be random, though they are depending on initial conditions. Therefore, the watermark is generated through messy algorithm by using the color plane as initial condition.

The initial values to the messy system is,

c_seq (a, 0) = k floor(s (a) /*2^l *)**2^l *+b* pos+c*key*

Where, s (a): pixel values of reference color plane of image.
k,b,c :predefine constant
l: embedding depth
pos: position information
key: secrete key
c_seg (a, 0):new sequence

The a^th pixel the sequence is referred as c_seq (a, i), i=l, 2, 3 ...l The number of repetition is performed for the a^th pixel to obtain the messy status. This type of sequence has the floating numbers that are converted in to binary sequence in the proposed scheme. Hence, apply threshold T is to convert the sequence c_seq (a, i) from floating to binary sequence w (a, i)[2].

The w (a, i) is obtained by

$$w(a,i) = \begin{cases} 1 \quad c\_seq(a,i) > T \\ 0\, else \end{cases}$$

Where, T: threshold value
a: pixel

D. *Reversible data hiding for pixel expansion*

Reversible data hiding techniques are *used* to *re*solve the problem of lossless embedding of large messages in digital images so after the embedded message is extracted, the image can be completely restored to its original state *as it is*. Tian devised a high-capacity reversible data hiding technique called difference expansion (DE), in which the resulting high-pass bands are the differences between adjacent pixel values.

For an *N*-pixel 8-bit host image *H* with a pixel value *xi* , where *xi* denotes the value of the *i*th pixel, $0 \le i \le N - 1$, *xi* ∈ **Z**, *xi* ∈ 0, 255.

1) Scan the image *H* in an inverse s-order. Calculate the pixel difference *di* between pixels *xi* −1 and xi by

$$\text{di} = \begin{cases} \text{xi , if i} = 0, \\ |\text{ xi - 1 - xi }|, \text{ otherwise} \end{cases}$$

2) Determine the peak point *P* from the pixel differences.

3) Scan the whole image in the same inverse s-order as in

Step 1. If *di* > *P*, shift *xi* by 1 unit

$$\text{yi} = \begin{cases} \text{xi , if i} = 0 \text{ or di} < \text{P}, \\ \text{xi} + 1, \text{ if di} > \text{P and xi} \ge \text{xi - 1}, \\ \text{xi - 1, if di} > \text{P and xi} < \text{xi - 1}, \end{cases}$$

where yi is the watermarked value of pixel i .

4) if *di* = *P*, modify *xi* according to the message bit

$$\text{yi} = \begin{cases} \text{xi} + \text{b, if di} = \text{P and xi} \ge \text{xi - 1} \\ \text{xi - b, if di} = \text{P and xi} < \text{xi - 1} \end{cases}$$

At the receiving end, the recipient extracts message bits from the watermarked image by scanning the image in the same order as during the embedding. The message bit *b* can be extracted by

$$\text{b} = \begin{cases} 0, \text{ if } |\text{ yi .- xi - 1}| = \text{P} \\ 1, \text{ if } |\text{ yi - xi - 1}| = \text{P} + 1 \end{cases}$$

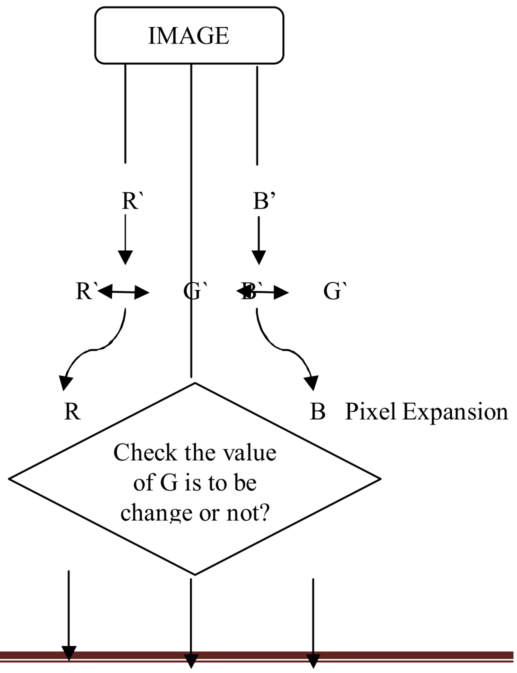
where *xi* −1 denotes the restored value of *yi* −1. The original pixel value of *xi* can be restored by

$$\text{xi} = \begin{cases} \text{yi} + 1, \text{ if } |\text{ yi .- xi - 1}| > \text{P and yi} < \text{xi - 1} \\ \text{yi - 1, if } |\text{ yi - xi - 1}| > \text{P and yi} > \text{xi - 1} \\ \text{yi , otherwise.} \end{cases}$$

Thus, an exact copy of the original image is obtained. These steps complete the data hiding process in which only one peak point is used. Large hiding capacities can be obtained by repeating the data hiding process.[4]

V. To Check Copyright of an Image

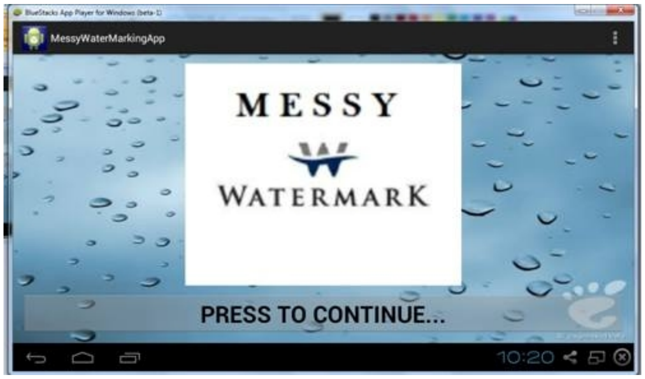
At the receiver side the image is modified or not is going to check by following procedure. This procedure is exact the opposite to that of watermarking except the checking the modified bits from original image.

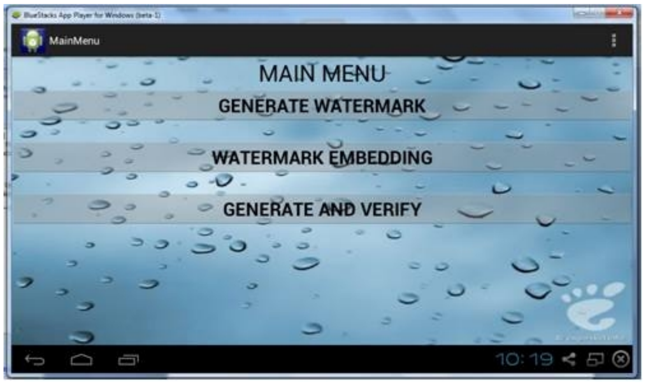


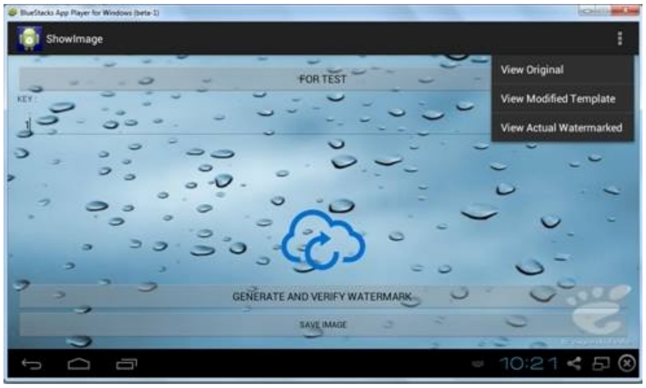
ORIGINAL IMAGE

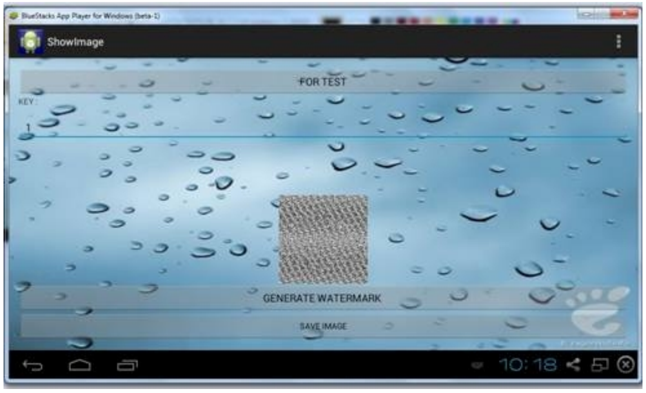
In this image the detail procedure is explain to check for copyright of an image. The main operation is to check the green plane is to be modified or not. If there is any change in green plane then there is something wrong with our image otherwise the image is totally secure from piracy.

VI. Experimental Results









VII. Conclusion

No one can changes the original images which are uploaded on internet. Watermark can be extracted without any type of loss of original image. Embedded watermark in the system would not be removed by commonly used image processing techniques. Original image is going through many embedding process, so it is hard to edit or making changes to it. The platform for this image is android because lot of people used this phone so anyone can load image for security purpose.

Acknowledgment

This is to acknowledge and thank all the individuals who played role in shaping this project report. Without their constant guidance and assistance this report would not have been completed. Their guidance, coordination and reviewing this task could not be completed alone. We avail this opportunity to express our deep sense of gratitude and hearted thanks to our guide Prof. P.M. Patil sir for giving his valuable guidance, inspiration and encouragement to embark this report.

References

[1] "Yueh-Hong Chen,Hsiang-Cheh Huang", "A Copyright Information Embedding System for Android
Platform in 2011 Seventh International Conference on Intelligent Information Hiding and Multi-
media Signal Processing", VOL.no{5, PP 60{70, March 2011.

[2] "S.Poonkuntran,R.S.Rajesh","A Messy Watermarking for Medical Image Authentication",vol. 7,
no. 4, PP 94-97,October 2008.

[3] "Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang","Reversible Data Hiding Based on His-
togram Modi_cation of Pixel Di_erences,IEEE Trans. on Circuits and Systems for video
technology", vol. 4, no. 8, PP. 12-19, june 2002.

[4] "Peipei Shi,Zhaohui Li,Tao Zhang","A technique of improved steganography text based on chaos
and BPCS", vol. 1, no.3, PP. 23-30, November 1999.

[5] "C.-T. Hsu and J.-L. Wu"," Hidden digital watermarks in images,IEEE Trans. Image Processing,
vol. 8, no. 1, pp. 58{68,January 1999.
3