COPYRIGHT PROTECTION FOR IMAGES ON ANDROID PHONES

Prashant Shinde[1], **Chetan Mohol**[2]

*[1, 2]Department of Computer Engineering, University of Pune, Zeal education society,
Dnyanganga collage of engineering and research, narhe- Pune*
7490pstshinde@gmail.com, chetan7253@gmail.com

Abstract

In the mobile device area, new advance features are introduced such as android phones, tablets, windows phones. Using this mobiles phones , we can capture the image and we can edit the image using some applications such as Photoshop on pc's .This type of phones also provide one feature like publish our image on websites. Hence, there is need a mobile application which provides protection to those images on mobile itself. There are some common approaches which guaranteed security to digital images is to use steganography and watermarking. We are trying to develop a tool for Android OS that permits to add watermark to images using BPCS algorithm. In this paper, we discuss this application and working of BPCS algorithm.

Keywords: – *Mobile image security, steganography, watermarking, copyright protection, bit plane, BPCS.*

---***---

1. INTRODUCTION

In an electronic device [1] like mobile (smart phone, tablet) increases their potential in terms of hardware and software. In mobile phones, some operating systems are available like android and symbian. There are many applications are available for this mobile and that are install on it.

Before some years back, these devices are used for only sending message, playing video/audio, internet browsing etc. Before so but now a day, smart phones are introducing with incredible changes such as image publishing etc. Some years back, these devices are used for only sending message, playing video/audio, internet browsing etc.

So, there is need to provide protection to images to avoid loss of information like as ownership information. Prevent images from those people which do not have any access permission. By using digital watermark we can embed the information into image. This technique is mostly use to identify the ownership of the copyright of such image. Watermarking means hide digital information in a image data. Digital watermark is use to verify the authentication of image or to show the identity of its producer.

The best solution is to embed the image watermarking information related to image itself or about producer company, website, etc. The steganography also use to provide protection of copyright images. Steganography is art or science of hiding the written messages inside the image in such a way that except sender and receiver, no one can recognize that message.

Both digital watermarking and steganography uses the steganographic techniques to embed data covertly in noisy signals. Since a digital copy of data is same as original, digital watermarking is a passive protocol tool. It only mark data, but does not degrade it not keep track on access to it.

One of the application of digital watermarking is source tracking. Later if the work copy found, then we can retrieve information (watermark) from copy and source of the distribution is known. Likewise we can detect the source of illegally copied images.

There are basically two types of watermark: visible water marking and invisible watermarking. Visible watermarks change the original information of the image which can be easily recognized by human eyes or any statistical analysis. Visible watermark means embedding the logos/trade marks in images. Example is shown in below fig.1. But now a day, to embed the information into image we use the invisible watermarking technique. This technique is more secure than visible watermarking technique.

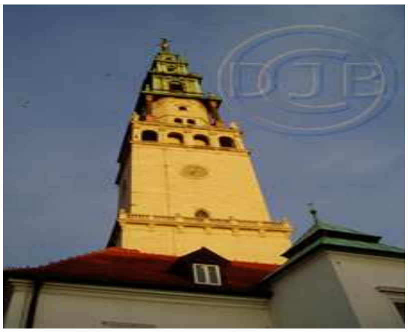

Fig 1: This above image is affected by visible watermark technique (watermark is the logo). [6]

Invisible watermark means embedding the image/other secretes information into images. This cannot easily recognize by human eyes or any statistical analysis.

The remainder of this work is organized as follows: in Section II author discuss about Digital Watermarking. In section III author is discuss about Steganography. In section IV author is discuss about BPCS algorithm and its working.

In Section V author present the tool, based on Android OS, and focus on the visible and invisible watermarking capabilities of this tool. In Section VI author will report the experimental results experimental results achieved by the tool, In Section VI author present the conclusions and highlight future work directions.

2. DIGITAL WATERMARK

Digital watermarking [5] technique allows to add hidden copyright information to digital audio, video, or image and documents. Such information is present in the form of bits which describing information about the author or any other information such as name, place, etc.

In Digital watermark one of the main concepts is copyright protection for images. This will prevent from unauthorized copy of digital media without the producer permission.
There are substantially two types of digital watermark:

1) Visible Watermark
2) Invisible Watermark

Watermark information is digital picture or video. Watermarking is a text or a simple logo, which identifies the owner of the multimedia data.

For example the logo which identifies a IPL cricket team can be considered as visible watermark.

3. STEGANOGRAPHY

Steganography [4] is art or science of hiding the written messages inside the image in such a way that except sender and receiver, no one can recognize that message.

Steganography is like cryptography but only one change is that cryptography hides only messages and steganography hides the messages as well as communicators information.

In this paper there is hiding of the message in more secure way by providing the encryption and decryption technique. In this there is a use of public key encryption technique in which sender and receiver having different keys.

In Steganography [4] replacing of bits of noisy pattern data with bits of different invisible information is done. This hidden information can be simple text, cipher text or even images.

4. BPCS ALGORITHM

Bit-Plane Complexity Segmentation [2] Steganography is new steganographic technique, which has large information hiding capacity. This algorithm replaces the complex bits of bit plane of color image which cannot recognize by human eyes or any statistical analysis.

Working of BPCS steganography [3] is as follows:
1) The carrier image is divided into 8 different Bit-Planes. All the bit-planes are divided into small pieces of the same size, which is called bit-plane blocks, such as 8 ×8. (Shown in fig. 2)
2) Calculate the complexity of every block. The Complexity is defined as the amount of all the adjacent Pixels that get different values (one pixel is 0 and the other is 1). The maximum possible value of the complexity is denoted as max C.
3) Setting the complexity threshold of the bit-plane Block is max _C, here α is a parameter. The bit-plane block whose complexity is larger than max _C is used to embed Secret information. The smaller the value of □□, the more Secret information can be embedded.□
4) Secret information is formed into bit-plane blocks. After checking the complexity, if the complexity of each plane is greater than threshold value (i .e. α_max). Then replace those bits using our secrete information bits. This will not affect on our image.
5) This process is done for all bit planes. After embedding information into our image then wrap all the bit planes. This will gives us new embedded image (shown in fig. 3).
6) Extracting process is same as embedding process up to splitting of planes, then we will check the complexity of each bit plane, if we found that, plane is complex then we will extract those bits. This will give us our secret information.

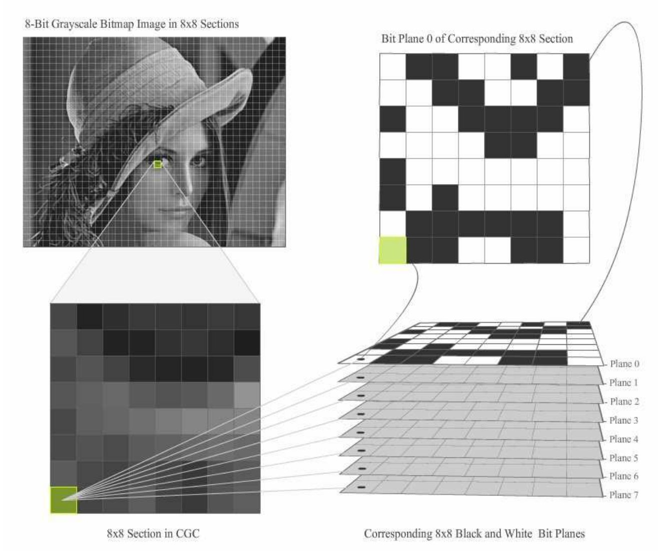
8-Bit Grayscale Bitmap Image in 8x8 Sections
Bit Plane 0 of Corresponding 8x8 Section
Plane 0
Plane 1
Plane 2
Plane 3
Plane 4
Plane 5
Plane 6
Plane 7
8x8 Section in CGC
Corresponding 8x8 Black and White Bit Planes

Fig2: bit plane separation [2]

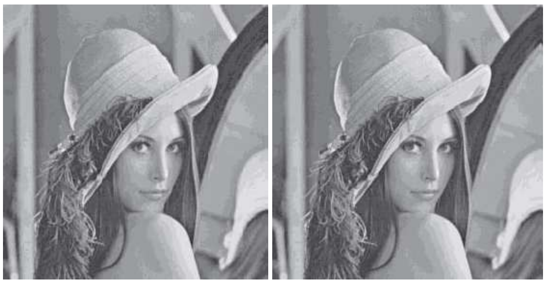

Fig 3: The image leena before and after steganography [2]

5. AN ANDRIOD OS WATERMARKING TOOL

We are trying to developed an android application for android OS(2.2 or later) That reads input image and affect it with watermarking (visible or invisible).

Supported file format are: .jpg, .jpeg, .bmp etc…

CONCLUSIONS AND FUTURE WORK

Due to the continue evolution of the mobile devices prompts us to investigate on the security issues. In particular, in this work it is considered the possibilities to guarantee the ownership of an image directly through the mobile devices.

We have proposed a application for Android OS that permits to add an invisible or visible watermark into an image.

Future work will consider the possibility to provide alert messages to the producer of images, if anyone made changes to the watermark image. Alert message include the information about which part of image is changed, at what time it is changed and from what location.

REFERENCES

[1] Raffaele Pizzolante, Bruno Carpentieri, "Copyright Protection for Images on Mobile Devices", Dipartimento di Informatica Università degli Studi di Salerno I-84084 Fisciano (SA), Italy, 2012

[2] Steve Beaullieu, Jon Crissey, Ian Smith," BPCS Steganography**",** University of Texas at San Antonio

[3] Peipei Shi, Zhaohui Li, Tao Zhang," A technique of improved steganography text based on chaos and BPCS", Nankai University, College of Information Technical Science Tianjin, China.

[4] "Steganography – Text/Image/Video/Audio Information Hiding". Available: http://electronicsbus.com/steganography-text-audio-image-video-security-information-hiding-cryptography.

[5]"http://www.watermark-software.com/resource/digital-watermarking.html

[6]."https://www.google.co.in/search?site=imghp&tbm=isch&source=hp&biw=1366&bih=600&q=visible+watermarking&oq=visible+water"