iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Image Piracy Alert System in Social Networks Using Watermarking

Saran R[1], Sujithra E[2], P. Yashwant[3], R. Vignesh[4]
[1,2,3,4]Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha University

Abstract— In this digital age one's content is growing in social networking sites. A novel technique has been proposed in this article to address this threat by using bit plane digital watermarking technique. A QR code representing the user is embedded in the user's image when, the theft of it is uploaded for the first time to prevent future unauthenticated usage in the social network. The QR code embedded using novel technique in order to withstand common image operations viz., cropping, brightness adjustment and noise addition.
Keywords— image security, QR code, social networking, watermarking

I. INTRODUCTION

Piracy is an increasing threat in social networking. Forge accounts are created by downloading profile pictures from original accounts. This is often unnoticed by the owner of the image. Watermarking is a versatile technique that has an edge over other techniques in the field of image processing in order to protect the user data from being misused. It provides copyright protection, integrity verification, content authentication and ownership proving [1-3]. However, implementing and embedding for more than one of these applications, it requires more than one watermarking. There are studies that report combined watermarking techniques that can implement a twofold application [4-5]. Digital watermarking techniques are classified as spatial watermarking and transform based watermarking [6-8]. The water marking technique was first coined by Andrew Tirkel and Charles Osborne in the year 1992 [9]. Extensive review studies give a better understanding of the watermarking concept and its techniques; the key factors determining the relevance of each technique attributed to it robustness, capacity, perceptibility and embedding method [10-12].
In this paper, watermarking and extraction is performed using Java. The digital watermarking is done using bit plane watermarking which is a spatial domain watermarking technique [13]. In this project, a program is developed to detect the image piracy and to alert the original owner about the piracy threat. When an image is uploaded in a social network, it is first checked for any previously written codes. If no digital codes are found it proceeds to the next step. A QR code is embedded into the image. The QR code contains the user ID of the uploader. When an attacker downloads this image and uploads in the same social network, the QR code is extracted and the user ID is read .There by alert information is sent to the original owner of the image. The alert message contains the details of the forge user ID.

II. OVERVIEW OF QR CODE

QR codes are used to encode and decode data at a quick rate[14]. QR code is basically a two dimensional square bar code by Denso Wave, in the year 1994 in Japan affiliated organisation known to be Toyota group. The QR code is a binary image consisting of square dots in white background having version information, format information, data and error correction key required patterns, position, alignment, timing, and quiet zone. The QR code is preferred to raw text because QR code can be fixed to a constant dimension. This feature makes it easy for the extraction. Another important advantage of using QR code is the facility of error correction. The ZXing package for Java is used for reading and writing QR codes.

III. BIT PLANE WATERMARKING

Bit plane watermarking is a spatial domain watermarking technique. In bit plane watermarking, the pixel values of the host image is explicitly altered corresponding to the watermark image, in such a way there is no perceptible change in the host image [15]. The changes in the least significant bits of an image cannot be perceived by human eyes, where the data is embedded.

IV. EMBEDDING

The QR code is embedded in the centre of the host image, so that the watermark is not tampered by cropping attacks. The LSBs of R, G and B bytes of the host image, is replaced by the 1-bit value of the corresponding pixel in the QR code. The 1 bit QR code is embedded in three bits of the 24 bit host image with bit mask 0x010101. Embedding the data in the centre of the image and in three bits of the host image is done with an intention which will be discussed later in attacks and error correction section.

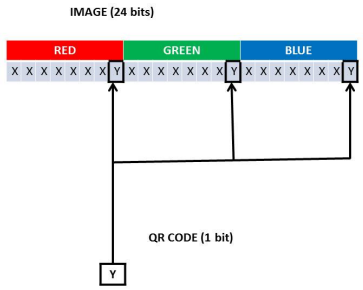


Fig. 1. Embedding QR code in the LSBs R,G and B bytes of image

V. EXTRACTION

The watermark is embedded in the centre of the image; hence the extraction is to be done in this region. The pixels of the watermarked RGB image is read with bit mask 0x010101. If the three bits i.e. the LSBs of the R, G and B bytes correspond to '1' it is taken as 'white' pixel and if the bits correspond to '0' it is taken as 'black' pixel. These extracted pixels are written into a separate file.

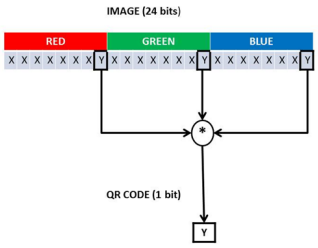


Fig. 2. The 1 bit QR code is extracted from the LSBs of R,G and B bytes

VI. WORKING PRINCIPLE

A user may be uploading a new image or an image which is saved from the social networking environment. When an user attempts to upload an image, there are two possible cases. However, in all the cases the program begins by extracting the QR code from the image. The extracted image is passed through a validation test to check if the photo is uploaded for the first time or it is uploaded by saving it from the social network. It should be noted that all the photos in the social network servers are watermarked with their corresponding QR codes.

A. Case 1: The user uploads a new photo

The extracted code is a noise image, because the LSBs of the R, G and B bytes have no embedded data. This fails the validity test for QR code. The read QRcode method provided by ZXing package throws the Not Found Exception. A QR code is generated by

passing the user ID to the write QR code method provided by ZXing package. This QR code is embedded into the centre of the image. When an user uploads an image which does not contain any QR code i.e., a new photo, it is watermarked. This process makes the user as the owner of the image he/she uploads. The upload is successful and the photo is made visible for all the users.

B. Case 2: The user saves another user's photo and uploads

The social network, allows a user to view another user's photo which is watermarked. And saving the photo is allowed by the browser from which the user logged in. But it is not reasonable for the user to upload other user's photo in the social network. The QR code is extracted from the image. This QR code corresponds to the original owner of the image. User ID is read from QR code using the read QRcode method. The user ID which is read is not equal to the user ID of the current user. Thus the image piracy is detected, an alert message containing the user ID of current user is sent to the user ID read from the QR code. The upload permission for the current user is also denied. If the user ID read is equal to the user ID of the current user i.e., the user save his own photo from the social network and uploading the same, the alert message is not sent and the upload is made successful.

VII. BLOCK DIAGRAM

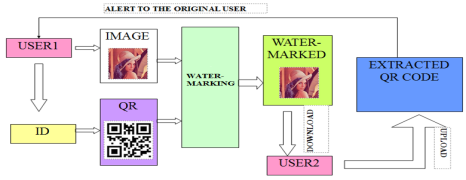


Fig. 3. Block Diagram showing the working principle.

VIII. ATTACKS AND ERROR CORRECTION

The watermarked image is publicly visible to all users in the social networking environment. Any user may download the image and tamper the watermark. A digital watermark should withstand the common image operations such as cropping, brightness/contrast adjustment, noise addition [16]. It should be possible to extract and read the data watermark successfully after these attacks.

A. Cropping

Since the watermark is embedded in the centre of the image, the data is not lost even if the corner of the image is cropped. Since the image is cropped the QR code is not available in the centre of the image. A Not Found Exception is thrown by the program when the QR code is extracted and attempted to read from the centre of the image. The QR code is searched in the watermarked image by extracting and reading throughout the image, till the end of file is reached or till the QR code is successfully read.

B. Brightness Adjustment

The brightness adjustment changes the values of the pixels implicitly. The brightness adjustment is mathematically represented as

$$p(i,j) = q(i,j) + B$$

p(i,j) is the pixel after adjustment at position i,j
q(i,j) is the pixel before adjustment at position i,j
B is the scalar which indicates the brightness adjustment

If the brightness is adjusted evenly in the R, G and B components of the image the QR code can be extracted. Thus the brightness adjustment will change the least significant bit of the R, G, B bytes of the image.

The LSB of the R, G and B bytes can take only two values either 'bit 1' or 'bit 0'. So there are two possibilities, extracting a QR code with black background and white foreground (when LSBs are inverted) and extracting a QR code with white background and black foreground (when the LSBs are not inverted). The former is the readable QR code while the latter QR code is to be inverted explicitly before reading.

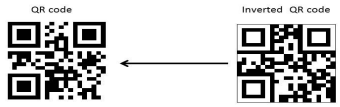


Fig. 4. Two possibilities of QR code after brightness adjustment

C. Noise Addition

In this case, random noise of small magnitude is unevenly added in the pixels of the watermarked image. The changes in the LSB values where the QR code is embedded is unpredictable. The three LSBs are extracted from the centre region of the image. In the three LSBs, the majority bit is taken as the watermark bit. If the number of 'bit 1' is greater than the number of 'bit 0' it is read as 'bit 1' and if number of 'bit 0' is greater than the number of 'bit 1' it is read as 'bit 0'. Further error correction is handled by the QR code read method provided by ZXing package.

IX. CONCLUSION

The proposed technique in this article provides security for the original contents in the social networking environment, by alerting the original content owners from image piracy threats. This technique also helps to identify the unauthenticated user thus making the internet world a safer environment.

REFERENCES

[1] Kaushik Deb,Md. Sajib Al-Seraj, Md. Moshiul Hoque, and Md. Iqbal Hasan Sarkar, "Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection", 2012 7th International Conference on Electrical and Computer Engineering 20-22 December, 2012, Dhaka, Bangladesh, 978-1-4673-1436-7/12/$31.00 ©2012 IEEE.

[2] G. L. F'riedman, "The 'Ikustworthy Digital Camera: Restoring Credibility to the Photographic Image", IEEE 7hns. Consumer Electronics, Vol. 39, pp. 905- 910, 1993.

[3] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", Proceedings of the IEEE, Vol. 87, pp. Table 1: Tampering evaluation of SPIHT. 1079-1107, 1999.

[4] Chun-Shien Lu, Hong-Yuan Mark Liao and Chwen-Jye Sze, "COMBINED WATERMARKING FOR IMAGE AUTHENTICATION AND PROTECTION", 0-7803-6536-4/00/$10.00 (c) 2000 IEEE.

[5] Stefano Chessa, Roberto Di Pietro, Erina Ferro, Gaetano Giunta, Gabriele Oligeri, "Mobile Application Security for Video Streaming Authentication and Data Integrity Combining Digital Signature and Watermarking Techniques", 1550-2252/$25.00 ©2007 IEEE.

[6] Jamal A. Hussein, "Spatial Domain Watermarking Scheme for Colored Images Based on Log-average Luminance", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 1, JANUARY 2010, ISSN 2151-9617.

[7] Mustafa Osman Ali , Elamir Abu Abaida Ali Osman, Rameshwar Row, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 5, November 2012

[8] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques" 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[9] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666- 673

[10] Vinita Gupta, Mr. Atul Barve, "A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

[11] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video", Proceedings of the IEEE, vol. 87, no. 7, pp. 1108-1126, 1999.

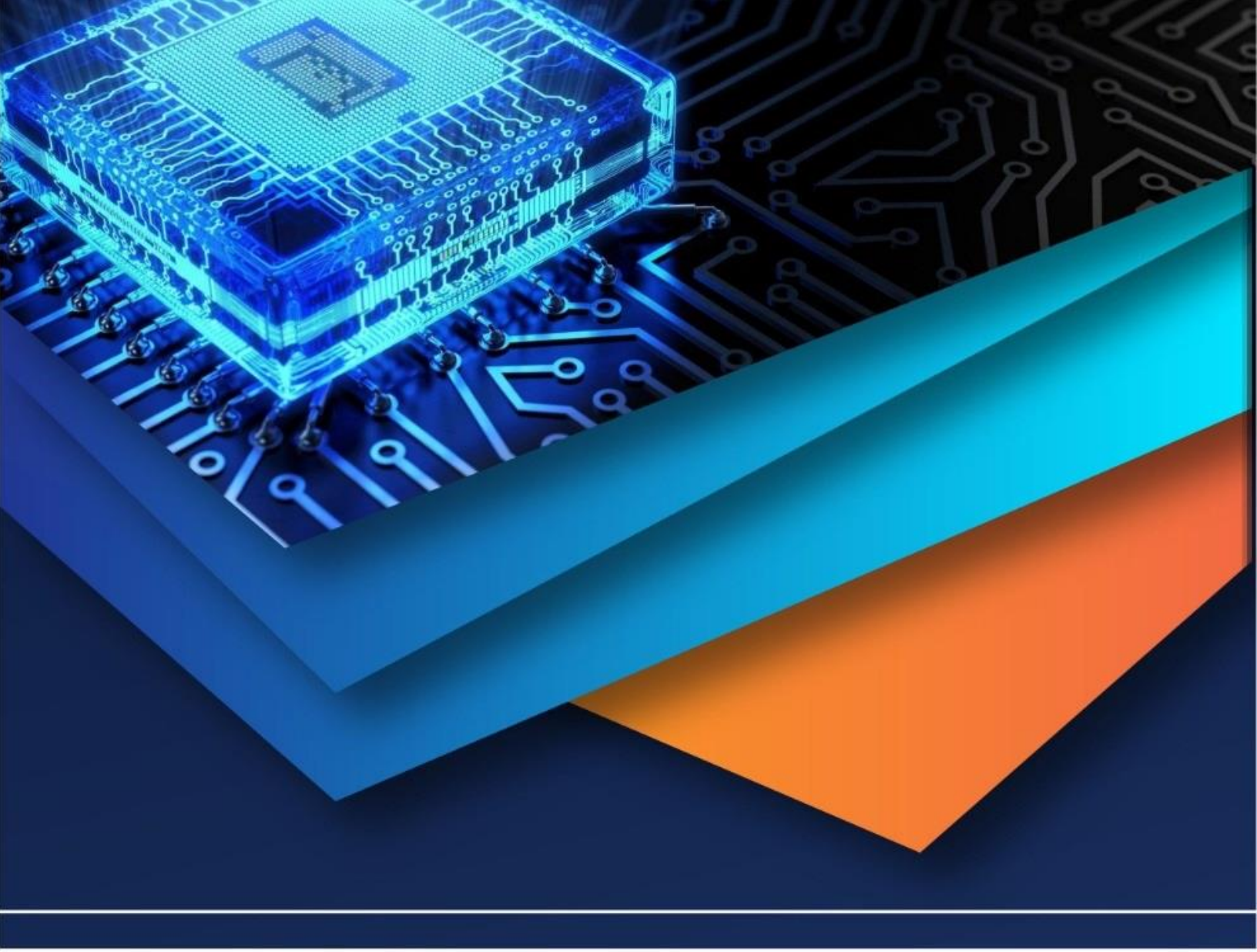
[12] Prabhjot Kaur Cheema, Kamaljit "Comparison of Text Watermarking Approaches with the Proposed Approach Based on Encryption Techniques used for Creating Watermarks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2014.

[13] Gwanggil Jeon and Young-Sup Lee, "Bit Plane Approach for Watermarking", SoftTech 2013, ASTL Vol. 19, pp. 211- 214, 2013 © SERSC 2013.

[14] Rouillard, J., "Contextual QR codes", Computing in the Global Information Technology, 2008. ICCGI '08. The Third International Multi-Conference, p. 50-55 E-ISBN 978-0-7695-3275-2.

[15] Akram M. Zeki and Azizah A. Manaf, "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit)", World Academy of Science, Engineering and Technology Vol:3 2009-02-23.

[16] Chuen-Ching Wang, Shen-Chuan Tai, Chong-Shou Yu, "Repeating Image Watermarking Technique by the Visual Cryptography", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E83-A No.8 pp.1589-1598.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY