ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 4, April 2014

Copyright Protection and Authentication of Image using Watermarking

Author: Prashant S. Dhotre[1]; Ankita Daga[2]; Sanman Borate[3]; Alankrita Khadtare[4]; Mayur Singhania[5]

Affiliation: [1, 2, 3, 4, 5] Sinhgad Institute of Technology and Science, Narhe, Pune-41

University of Pune, India

ABSTRACT

The expansion of the Internet has frequently increased the availability of digital data such as audio, images and videos to the public. Digital watermarking is a technology which is used in the public. Digital watermarking is a technology to ensure and facilitate data authentication, security and copyright protection of digital media. This paper proposes watermarking scheme for authentication and copyright protection of images. The images that are used are in RGB color space. The proposed scheme is dual watermarking scheme which dynamically generates the watermarks and embeds them inside the image instead of single watermarking scheme process only. The dual watermarking scheme adds to the effectiveness of system. In this approach with the help of both watermarking schemes we try to ensure the copyright protection of image from unauthorized use in a better way.

Keywords

Copyright, image watermarking, image authentication, α-channel.

1. INTRODUCTION

With the rapid advancement of network technology, multimedia information is transmitted over the internet conveniently. Whenever an image is shared or exchanged within some network it may be possible that the image may be used without the permission of the owner. To deal with the security problems of copyrighted images, various image data hiding schemes have been developed. Copyright protection and authentication have been the most important issues in the digital world.

Copyright tells us about the real owner of the image in similar manner authentication tells that if the image has been damaged or not. Recent research has pointed to steganography and digital watermarking as two areas which are generally referred to as information hiding. Steganography is the hiding of a secret message within an ordinary message and its extraction at a destination [1].Digital Watermarking, as opposed to steganography, has the additional requirement of robustness against possible attacks [1].The purpose of digital watermarking is to provide evidence that can be used within the legal system to prove that some copyright protection violation has occurred [2].The goal is to give the copyright owner of a digital of a digital image (or other piece of information) the possibility to prove technically the origin of the image. Watermarking does not address authentication explicitly. They are used for authentication in special applications and are usually designed to resist alterations and modifications [3].

2. RELATED WORK

Literature survey on past paper of watermarking is discussed below:

Jun Tian, [4] partitioned image into pairs of pixel values, select expandable difference numbers for difference expansion and embed a payload which includes an authentication hash. By exploring the reversibility is achieved. In this it do not need to compress original embedding area. The final restored image will be identical to the original image pixel, bit by bit.

Adnan M. Alattar, [5] a very high capacity algorithm based on the difference expansion of vectors of an arbitrary size has been developed for embedding a reversible watermark with low image distortion. Test results of the spatial triplet-based and spatial quad-based algorithms indicate that the amount of data one can embed into an image depends highly on the nature of the image. To maximize the amount of data that can be hidden into an image, the embedding algorithm can be applied recursively an across the color components. It does not support if the image is highly distorted.

R. Schyndel, A. Tirkel, and C. Osborne, [6] generated a watermark using a m-sequence generator. The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark was extracted from suspected bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. Schyndel showed that the resulting image contained an invisible watermark with simple extraction produces. The watermark was not robust to additive noise.

3. PROPOSED SYSTEM

The proposed system consists of dual watermarking scheme for better security of the image. It is divided into four phases.

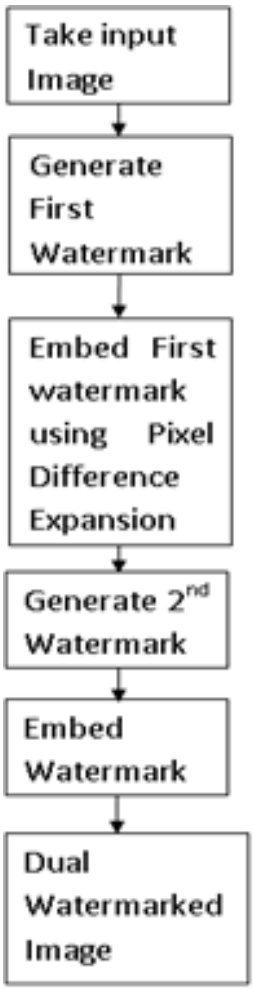

Fig 1: Basic flow of proposed system

Fig 1.shows idea about the flow of proposed system and also shows the steps to achieve dual watermarking.

3.1 Generate the First Watermark

In this phase, we take the basic image as input to the system. We split the given image into the bit planes (i.e. each pixel of the image is of 24-bit) and we divide it in 3 different bytes of RGB color. Then we take reference plane whose least significant bit of every pixel in the image would be used to produce the watermark that is needed for embedding [1] (i.e. we store the least significant bit values for every pixel for a reference plane and use it as watermark. As every image might have different least significant bit values it would help us producing the watermark in dynamic way. We will not be considering the reference plane for pixel difference expansion, the other two planes will be considered for pixel difference expansion.

Fig 2: Generation of first watermark using green plane as reference plane for image of Lena

Fig 3: Watermarked image of Lena

3.2 Encrypt and Embed the Produced Watermark with the help of Pixel Difference Expansion

The watermark generated in previous stage will be embedded in this stage by using pixel difference expansion as shown in Fig 4. The watermark generated in last phase is dynamic and is unique for image chosen for watermarking. In this phase we encrypt the watermark with the help of some external key. The key can also be used to extract the watermark and is external. With the help of encryption algorithm and external key, encrypted watermark is produced. Now the encrypted watermark generated at this stage is embedded within the image with help of pixel difference expansion. The reference plane is kept constant while the other two planes are expanded and the encrypted watermark is embedded i.e. if green color plane will be used as seed to generate the watermark the pixel pair is formed from the red and blue color planes of the image [5]. By checking if the pixel can be expanded or not condition for every pixel pair, the encrypted watermark is embedded in the difference as shown in the Fig 4.

$$m = [(x + y)/2] \quad (1)$$

$$D = x - y \quad (2)$$

Where m is integer average and D refers to difference. x and

y are pixel values for unreferenced plane.

After hiding this encrypted watermark we are done with the embedding of first watermark can be done in exact inverse way.

The inverse can be done as follows:

$$X=m+ [(D+1)/2] \quad (3)$$

$$Y=m- [D/2] \quad (4)$$

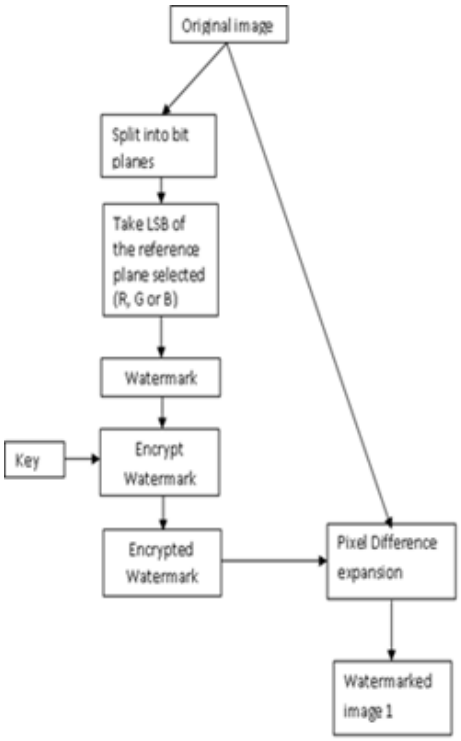

Fig 4: Generation of α-channel and embedding it in image

3.3 Generation of Second Watermark (α-channel)

After embedding the first dynamically generated water-mark with the help of pixel difference expansion in the image, the resultant image in this phase is again split the given image into red, green and blue planes. We here use the concept of the α-channel. This watermark is again dynamic and is unique, as it is generated from the pixels of the image again. Here, what we do is, we generate α-channel with the help of the red, green and blue values of all pixels. The aver-age of the RGB values for every pixel in the image is found out for the generation of the α-channel. The α-channel consists of average of red, green and blue values for all pixels in the provided image. This α-channel acts as verification in-formation to find out if the image has been or has not been damaged in unauthorized use.

$$(R+G+B)/3 \quad (5)$$

It is calculated for all pixels in the image in order to produce the α-channel.

3.4 Embedding of α-channel

In this phase the α-channel generated within the last phase is embedded within the already watermarked image, along with the undistributed red, green and blues values of the every pixel of the image as shown in Fig 5. This watermark is again unique and dynamic for the image. The values of the pixel are kept undistributed in the image because the image should not be affected because of the watermark produced in the last phase i.e. if the image is damaged be-cause of the watermark then it would not be of any use in this case. This phase produces the image with dual watermarking. Now the dual watermarked image consists of both watermarks i.e. first watermark produced with help of reference plane's least significant bit values and the second watermark generated within the last phase.

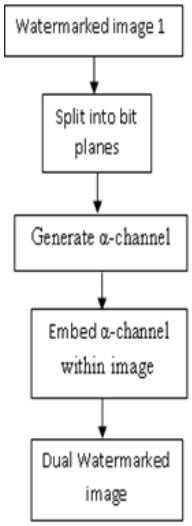

Fig 5: Generation of α-channel and embedding it in image

3.5 Watermark Extraction and Authentication of the Image

In the extraction process, the watermarked image is processed in the same way as original image processed for embedding. The extraction process is completely independent of the watermark [5, 6, and 7]. Both original image and original watermarks that have been embedded are not used in the extraction process. This process is used to detect if the image has been damaged or not in case of unauthorized use. In this phase we check if the image has been damaged or not with the help of the two watermarks that we have embedded as proposed in this paper. As the α-channel is embedded in second phase. In the first phase of extraction we check the image has been damaged or not with help of the α-channel embedded. The average of the pixel values of the given image will be compared to α-channel. If

the average for pixel values has been damaged it would simply detect that the image has been damaged. We will be extracting the α-channel and comparing it with the current α-channel average pixel values so as to find out the damaged pixels of the image. If we cannot detect any changes with the help of α-channel then we try to detect the changes with help of extracting the first watermark using pixel difference reduction. In the second phase of watermark extraction and authentication i.e. if we cannot detect any changes with the help of α-channel then we will extract the first watermark embedded with the help of pixel difference reduction and also generate the watermark with help of reference plane of the image that is provided to system. We will compare both the watermarks and if they both match the conclusion would be image has not been damaged otherwise it would detect that the mage has been damaged.

4. EXPERIMENTAL RESULTS

In first phase of watermarking, watermark is stored only in some pixels and in second phase of watermarking, metadata of all pixels are stored. Depending on number of expandable pixels, tampering can be detected in verification process of first phase of watermarking.

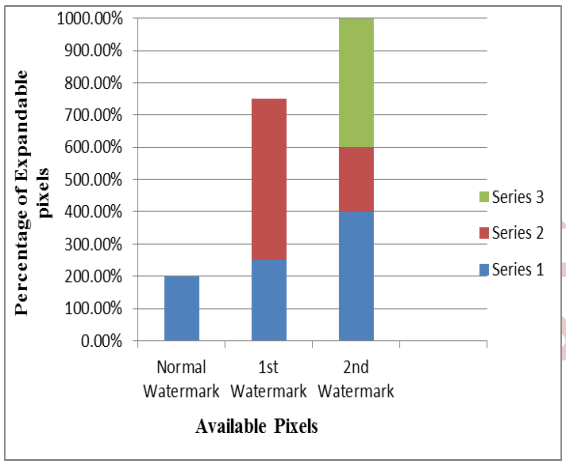

Fig 6: Expandable Pixels VS Available Pixels

5. CONCLUSIONS

The proposed method uses dual watermarking scheme for copyright protection of image and image authentication. It generates both the watermarks dynamically. The watermarks generated are unique to image. We are embedding the first watermark with help of pixel difference expansion of other planes than the reference plane and the second watermark would be containing the average of the pixel values of image. The system would be able to produce better results than the systems proposed earlier as it uses dual watermarking and thus, help us to protect the image from its unauthorized use.

6. ACKNOWLEDGMENT

We are thankful to our department and our guide Prof. Prashant S. Dhotre for supporting us to develop this template.

7. REFERENCES

[1] S.C. Katzenbeissar and F.A.P. Petitcolas (Eds.). "Information Hiding Techniques for Steganography and Digital Watermarking" Norwood, MA: Artech House, 2000.

[2] S.Poonkuntran and R.S.Rajesh "A Messy Watermarking for Medical Image Authentication" 2011 IEEE.

[3] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn. "Information Hiding- A Survey" Proceedings of the IEEE, 87(7):1062-1078, 1999.

[4] Jun Tian, "Reversible Watermarking by difference expansion".

[5] Adnan M. Alattar, "Reversible Watermarking using Difference Expansion of a generalized Integer Transform", Image Processing, IEEE Transactions on volume: 13, Issue: 8, Digital Object Identifier, Publication Year: 2004, Page(s): 1147-1156.

[6] R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," Proc. IEEE Int.Conf. On Image Processing, Nov. 1994, vol. II, pp. 86-90.

[7] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, Fellow, "Reversible Data Hiding Based on Histogram Modification of Pixel Difference" 2009 IEEE.