A Visual Cryptography based scheme for Digital Watermarking of Colour Images

Shwetha Ram
Department of Electrical and Electronics Engineering,
National Institute of Technology Karnataka, Surathkal.
+91-9741851969
shwetharam0407@gmail.com

Carmen Angeline Goveas
Department of Electrical and Electronics Engineering,
National Institute of Technology Karnataka, Surathkal.
+91-8892567337
goveas.carmen@gmail.com

1. INTRODUCTION

As technology progresses and more and more personal data is digitized, there is a greater emphasis on data security today than ever before. Keeping this data safe and secure in a way that does not impede its access by any authorized person(s) is an immensely difficult and very challenging research problem. In this paper, we propose a scheme for the digital watermarking of colour images based on Visual Cryptography.

According to the proposed scheme, the verification information is generated using the image to be marked, a watermark and a passkey. The watermark and the verification information are registered with a neutral authority. The owner of the image is in possession of the passkey which he must provide to validate an ownership claim. Using the test image, passkey and verification information, it is possible to generate the watermark which should match the original if the claim is true.

This method works on a random selection of pixels generated by using the passkey as the seed. The algorithm is based on the relationship between the randomly selected pixels and their nearest neighbour pixels. Even if the most significant bits of some random pixels have been changed, the technique is robust enough to handle such attacks.

The marked image is in all respects identical to the original image.

2. BACKGROUND AND RELATED WORK

Visual Cryptography was first proposed by Naor and Shamir as a cryptographic technique which allows visual information such as text, pictures, etc., to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. It provides a very powerful technique by which one secret can be divided into two or more shares. This basic technique, now known as '**Traditional Visual Cryptography**', has been improved and augmented in many ways. In **'Extended Visual Cryptography'**, it is attempted to give meaningful shares instead of choosing them randomly. **'Dynamic Visual Cryptography'** aims at multiple secret sharing, i.e., hiding more than one piece of information within a set of shares. Another important direction for the growth of visual cryptography was extending to gray scale and colour images. As more and more data is confined to a digital platform, many algorithms have come up which work on the underlying concept of sharing secrets into many shares but do require a computer for decryption. However, this is not a drawback for many applications today.

Visual Cryptography has many applications in areas like image hatching, moiré patterns, anti-phishing of websites, user authentication, home security, watermarking and copyright protection. This paper deals with one application of visual cryptography, i.e, digital watermarking of images, modifying A.H.Abusitta's idea for digital watermarking of grayscale images and providing an extension to colour images as well.

3. APPROACH AND UNIQUENESS

The algorithm for generating the verification image for any colour image using a binary watermark and a passkey works as follows. The image to be marked has its red, green and blue streams separated to get three gray scale images. The image of the watermark is divided into three parts. Using one part of the watermark, one stream of the image and the passkey, three sets of verification information are generated using the algorithm for gray level images described in section 3.2. The verification image generated from red stream becomes the red stream of the final verification image and likewise for the green and blue streams.

While authenticating an image, the verification image has its red, green and blue streams separated. Each of these streams is used with the passkey and the three streams of the test image to yield the corresponding watermark using the algorithm described in section 3.4. Now, the three watermark images so obtained are added to get the final watermark image which is then compared with the original.

3.1 Algorithm for generating Verification Information given the Original Image, Passkey and the Binary Watermark

- ➢ Read the original image img
- ➢ Read the watermark wmk
- ➢ Separate the 24-bit image img into red, green and blue streams to get three gray level images
- ➢ Divide the watermark wmk into three binary images
- ➢ Using one watermark image and one gray level image for a given passkey as illustrated in section 3.2, generate three verification images.

- These form the red, green and blue streams of the final verification image.

3.2 Algorithm for generating Verification Information given a Gray-level Image, Passkey and the Binary Watermark Image

- Read the original image img
- Read the watermark wmk
- Read size of img [R ,C]
- Read size of wmk [r,c]
- Using the passkey as a seed generate r*c random numbers between 1 and R*C
- Let the array of random numbers be a.
- For every a_i
    - More = No of pixels among the 8 nearest neighbours of img(a_i) whose intensity value is greater than img(a_i)
    - Less = No of pixels among the 8 nearest neighbours of img(a_i) whose intensity value is less than or equal to img(a_i)
    - If less≤more && wmk(i)==1, V=[1 0]
    - If less>more && wmk(i)==1, V = [0 1]
    - If less ≤ more && wmk(i)==0, V = [0 1]
    - If less>more && wmk(i)==0, V = [1 0]
- The verification information V of all pixels is combined to form the verification image of size [r, 2*c]

3.3 Algorithm for generating Watermark given the Test Image, Passkey and the Verification Information

- Read the test image img
- Read the verification image
- Separate the test img into red, green and blue streams
- Separate the verification image into the red, green and blue streams
- Using verification image and test image of each stream as illustrated in section 3.4, generate three watermark images
- Add the three watermark images to obtain the final watermark image

3.4 Algorithm for generating Watermark given the Gray-level Test Image, Passkey and the Verification Information

- Read the test image img
- Read the verification information V from the verification image
- Read size of img [R ,C]
- Read size of verification image [r,2*c]
- Using the passkey as a seed generate r*c random numbers between 1 and R*C
- Let the array of random numbers be a.
- For every a_i
    - More = No of pixels among the 8 nearest neighbours of img(a_i) whose intensity value is greater than img(a_i)
    - Less = No of pixels among the 8 nearest neighbours of img(a_i) whose intensity value is less than or equal to img(a_i)
    - If less≤more && V ==[1 0], wmk(i)==1
    - If less>more && V == [0 1], wmk(i)==1
    - If less ≤ more && V = [0 1], wmk(i)==0
    - If less>more && V = [1 0], wmk(i)==0

- The image wmk is now compared with the original watermark for authentication.

4. RESULTS AND CONTRIBUTIONS

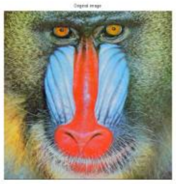

Fig. 1

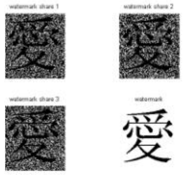

Fig. 2

Fig. 3

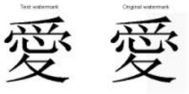

Fig. 4

4.1 Results

Fig.1 is the original image which is to be marked. In Fig. 2, we see the binary watermark which is split into three images. The verification image is shown in Fig. 3. A test image is generated by slightly deteriorating the quality of Fig. 1 and the watermark is regenerated using this test image, verification image and the passkey. This is recognizable as the original watermark as seen in Fig. 4.

4.2 Contributions

The existing algorithm for digital watermarking of gray-level images is extended to colour images and satisfactory results are obtained. As the method is based on a random selection of pixels based on the passkey, it is robust and capable of withstanding attacks to image quality. Further, it is not possible to recover the watermark from a test image that does not originate from the marked image.

Github link: https://github.com/shwetharam0407/A-Visual-Cryptography-based-scheme-for-Digital-Watermarking-of-Colour-Images

5. REFERENCES

[1] ‘A Visual Cryptography Based Digital Image Copyright Protection’,Adel Hammad Abusitta, Journal of Information Security, March, 2012.

[2] Image Captcha Based Authentication using Visual Cryptography, Mrs. A. Angel Freeda, M.Sindhuja, K. Sujitha, IJREAT April- May, 2013

[3] 'Visual Cryptography for Colour Images', Young- Chang Hou, The Journal of The Pattern Recognition Society, June, 2002

[4] 'Protecting Digital Media Content', Nasir Memon and Ping Wah Wong, Communications of ACM , July , 1998.

[5] ‘Visual Cryptography’, Moni Naor and Adi Shamir, Eurocrypt 1994.

[6] An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications, Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam and Tanveer Al Jami, International Journal of Computer Applications, March, 2013

[7] ‘Visual Cryptography and its Applications’, Jonathan Weir and Weiqi Yan, Ventus Publishing Aps