International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 4 Issue 6|| June 2015 || PP.07-13

Digital image copyright protection based on visual cryptography

[1,] Prof.A.B Ingole, [2,] Kranti Vikram Patil, [3,] Bhagyashree Ramnath Rajpure
[1, 2, 3,] Dept of ENTC Engg.
Savitribai Phule Pune University Pune-48, India

ABSTRACT—*The system proposes a simple and efficient watermark based on visual cryptography. Visual cryptography deals with visual information (pictures, text, etc.) to be encrypted into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. In the proposed method, data is extracted and stored as one share of the watermark pattern instead of embedding data into the original image as in the conventional watermarking schemes. We know that the watermark method is an excellent technique to protect the copyright ownership of a digital image. The watermark pattern can be any black and white image used to typify the owner. Since no data is embedded, the method is robust against watermark attacks and the watermark pattern is very difficult to detect and remove in an illegal way. It can be retrieved from the marked image without making comparison with the original image. The notary also can off-line adjudge the ownership of the suspect image by this method Experimental results show that the method is robust even in the case of maximum frame drop.*

INDEX TERMS— *Visual cryptography, Encryption, Decryption, Image watermark, Verification Information, copyright protection.*

I. INTRODUCTION

With the increasing convergence of network, services, and devices, more number of end user devices is accessing digital media content which was hitherto accessible mainly from computers and television sets. The rapid growth of digital media such as Internet and CD's has made the digital images easy to distribute, duplicate, disturb and modify.This makes the digital media more prone to illegal copying and distribution.Images are susceptible to various other attacks like JPEG compression, sharpening, lightening, darkening, noising, blurring, distortion, rescaling, rotation, cropping, jittering, and mosaic attacks.In such cases an image watermark method is now drawing the attention as a good technology of protecting copyrights for digital data. The watermark pattern can be either visible or invisible. The applications of visible watermark are limited and it also distorts or changes original image pixels.[1][3]

There are several research articles exploring various watermarking methods. Some methods hide watermark in spatial domain [5] and some embed watermark pattern in frequency domain. However, these watermark methods are not transparent and robust and watermark pattern can be easily removed from them. In 1994, Naor and Shamir [2] proposed the concept of visual cryptography. By their method, an image can be broken up into n shares and shared image can be reconstructed by stacking some authorized shadow images without performing any computation. Any subset of unauthorized shadow images cannot infer any knowledge about the shared image. So here, we propose a robust digital image watermarking scheme for copyright protection using the principles of visual cryptography.According to the proposed method, the watermark pattern does not have to be embedded into the original image directly, which makes it harder to detect or recover from the marked image in an illegal way. It can be retrieved from the marked image without making comparison with the original image. The notary also can off-line adjudge the ownership of the suspect image by this method.

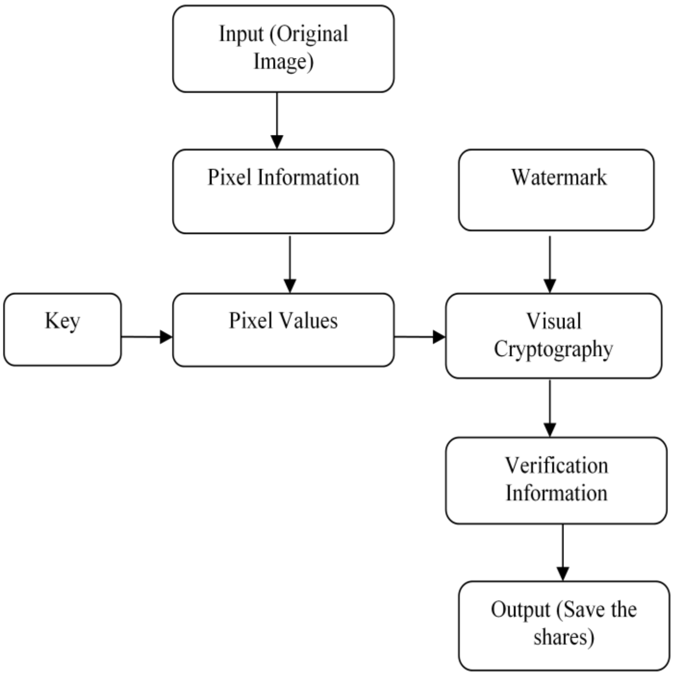
II. PROPOSED SYSTEM

We proposed a system which based on the simple (2,2)-visual threshold scheme .In earlier times papers proposed on visual cryptography had drawback, It was possible for hacker to extract watermark from image. We are introducing here new system that is image copyright protection using visual cryptography. Here we don't embed watermark directly into image indirectly it won't disturb our original image. By using watermarking method we secure our copyright .Watermark may be any threshold image. New concept introduced here is key which will randomize pixel of image hence it will be difficult for hacker to extract watermark image.

Shares we obtained is nothing but the visual information. Once we get 2 shares of image ,its important to submit key as well as shares to notary .Its not possible to retrieve watermark image back without key and only one part of share.

III. SYSTEM ARCHITECTURE

There are mainly two steps we are going to follow for digital image copyright protection. One is Encryption and other is Decryption. The respective block diagrams are as shown below:



Encryption Process

It consists of following eight blocks which are as explained below-

Original Image: Original image is nothing but a RGB image in which each pixel of image has 3 dominant colors that is red, blue green. As cryptography can't be performed on RGB images it is very necessary to convert this colored image to grayscale.

Pixel Information: Here we used average method for conversion as it is supposed to be easiest method to convert RGB into grey scale image. It just counts the sum of R,G and B pixels and then divide it by 3 to calculate the average. That average value is assigned to respective pixel. After averaging all pixels, our original RGB image gets converted into grey scale image.

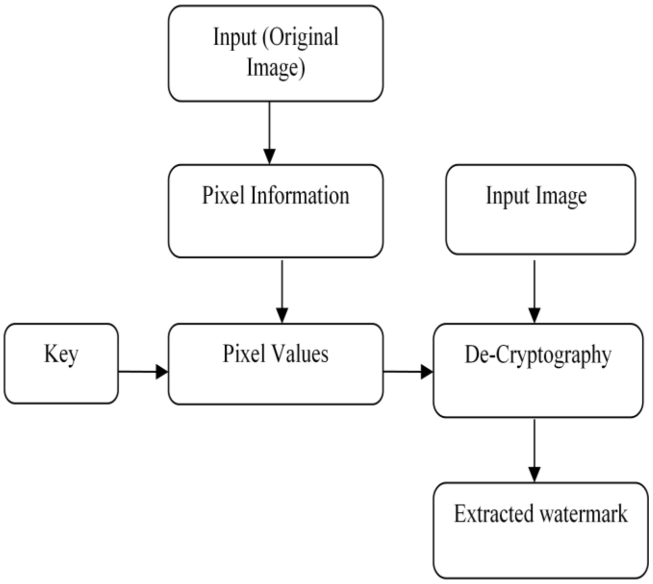
Pixel Value: The value of pixels of that grey scale image is what we called as 'pixel value' in block diagram. As the 24 bit is converted into 8 bit greyscale image, the pixel values are in 0's or 1's.

Watermarking: It is the method where we select any image as a watermark for our project. In order to use watermark its necessary to convert watermark image into threshold image.

Visual Cryptography: Visual cryptography is nothing but breaching of images into two shares such that you can't obtain original image back until and unless you have two shares. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images.

Key: Key is nothing but the secret password whose value will be known to image's owner. This key has to be has to keep secretly in order to ensure security for your own copyright. Without this key and verification information you won't be able to retrieve the watermark image back.

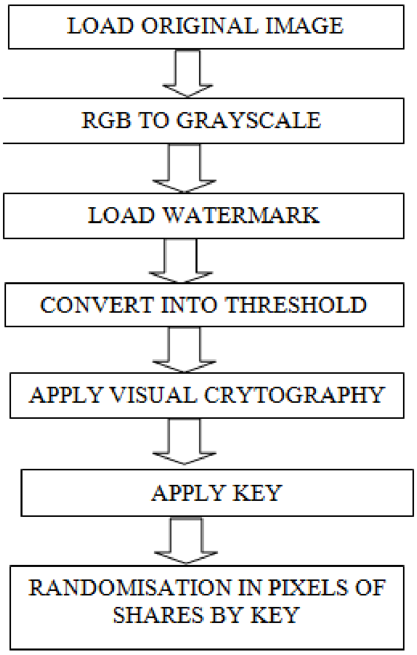
Verification Information: The verification information is nothing but the shares of the image to be protected which are obtained with the help of visual cryptography. The verification information will be registered in notary and it will be needed at the time of verification.



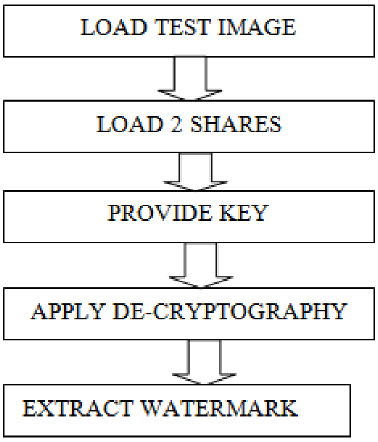
Decryption Process

De cryptography:
This is nothing but the inverse of visual cryptography. For applying de-cryptography, one has to refer pixels in 2 shares and original image. By knowing those pixel values, one can construct the pixel matrix of watermark.

A. Flow chart for encryption



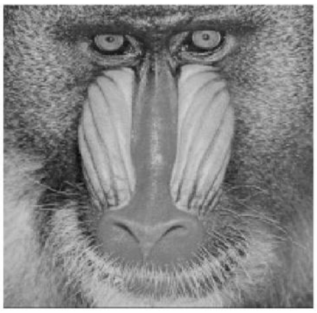
B. Flow chart for decryption



IV. RESULTS

A. RGB to Grayscale Conversion of Original Image

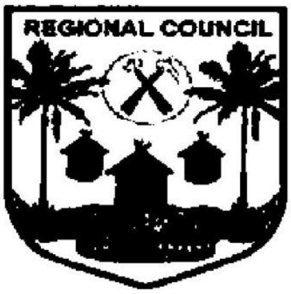
For applying visual cryptography, the original RGB image is converted into grayscale image. The RGB image is 24 bit image. It has to be converted into 8 bit by applying greyscaling. The conversion took place by averaging R, G and B component of each pixel i.e. (R+G+B)/3. The resultant value is of 8 bit which is having various shades of grey color. The results obtained are as follows.



Original Input image Grey-Scale image

B. RGB to Threshold Conversion of Watermark

The proposed system is based on the simple visual cryptography scheme in which he owner should select a black/white image as her/his watermark pattern. So if we select an RGB image as watermark, we have to convert it in threshold image. The size of watermark image should be less than the size of original image. The threshold image has only black and white pixels and the results are as shown below.

REGIONAL COUNCIL
OSHIKOTO


Watermark image Threshold of watermark

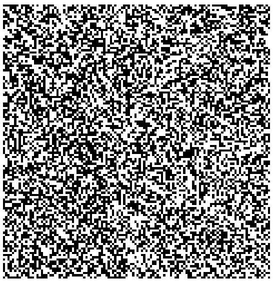
C. Encryption (Share generation)

For encryption process we have to perform following steps.

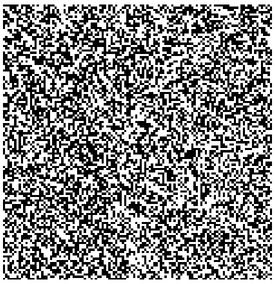
- Take 1st pixel of threshold of watermark image.
- Take MSB of 1st pixel of grey scale version of original image.
- By the combination of these two pixel, select the proper pair of verification information (Vi1, Vi2) , from the table given below

i-th pixel of watermark	The MSB of i-th pixel of image M is	Assign the i-th pair(Vi1,Vi2) of verification information to be
Black(0)	1	(0,1)
Black(0)	0	(1,0)
White(1)	1	(1,0)
White(1)	0	(0,1)

- Assign 1st bit(Vi1) to the 1st pixel of share 1. Assign 2nd bit(Vi2) to the 1st pixel of share 2.
- Follow the same procedure for all pixels to generate the 2 shares.
- Then apply a key to the system. The pixels will be randomized according to the ASCII value of the key.
- Suppose, ASCII value of key is 200, then 1st pixel of share 1 and share 2 will go to 200th position, 2nd pixel will go to 400th position and so on. So we get the 2 shares as follows.



Share 1



Share 2

The 2 shares generated are having random 1's and 0's only and they do not show any pattern so visually one cannot predict the watermark from these 2 shares. The owner should keep the key secretly to himself and produce the key and 2 shares at the time of verification.

C. Decryption(Extraction of watermark)

For extraction of watermark, we have to follow the steps:

- Take the 1st pixel of image under test.
- Take 1st pixel of share1 and 1st pixel of share 2.
- From the combination of those 2 pixels of share 1 and share 2 and MSB of original image, choose appropriate value of watermark from table given in encryption.
- Follow the same procedure for all pixels of the image under test. It'll give the extracted watermark.

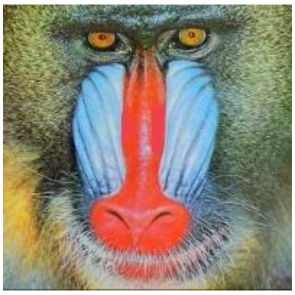
REGIONAL COUNCIL

Extracted watermark

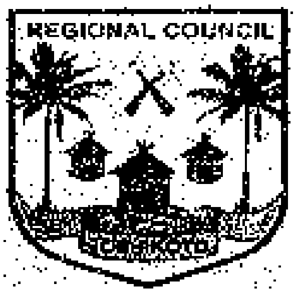
V. CONCLUSION

Visual Cryptography method has been proved to be excellent method to protect copyright ownership of image by using watermarking in it. Watermark image is any significant black and white image that is used to typify the owner.

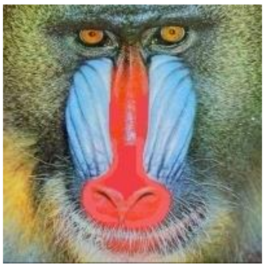
In visual cryptography we do not embed watermark pattern into image directly. It's highly impossible to recover watermark pattern back from one share. By making the use of secret key we randomize the positions of pixels which will randomize the pixels. Without secret key and shares its difficult to retrieve watermark pattern back.



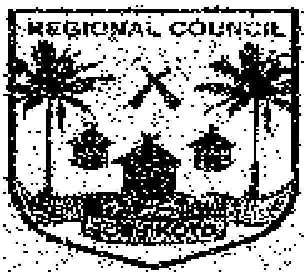
10% disturbed image



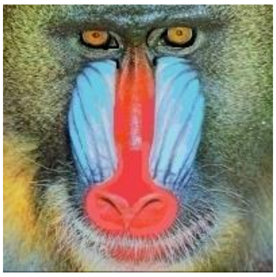
Extracted watermark



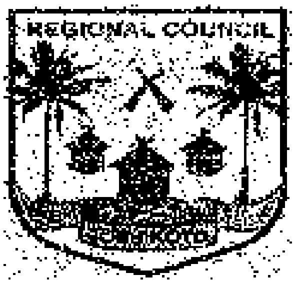
20% disturbed image



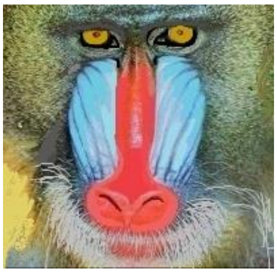
Extracted watermark



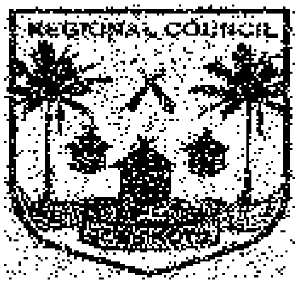
30% disturbed image



Extracted watermark

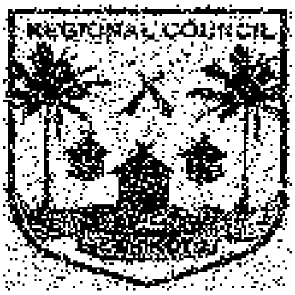


40% disturbed image



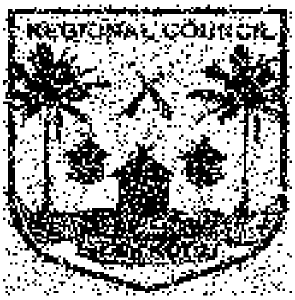
Extracted watermark

50% disturbed image



Extracted watermark

60% disturbed image



Extracted watermark

REFERENCES

[1]. Ms. Kiran kumara.2.Shalini Bathiya "Multi-pixel Visual Cryptography for color images with Meaningful Shares"International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2398-2407

[2]. Moni Naor and Adi Shami "Visual Cryptography" Department of applied maths and computer science, Weizmann Institute, Rehovot76100, Israel.

[3]. Bender W., Gruhl D., Morimoto N. and Lu A., "Techniques for Data Hiding," IBM System Journal. Vol. 35, No. 3, pp. 313-336 (1996).

[4]. Braudaway G. W., Magerlein K. A. and Mintzer F., "Protecting Publicly-available Images with a Visible Image Watermark," In the Proceedings of SPIE, Vol. 2659, pp. 126-133(1996).

[5]. Cox I. J., Kiliant J., Leighton T. and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687(1997).