



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

COPY RIGHT PROTECTION OF DIGITAL IMAGES WITH DIGITAL WATERMARK

1 A. Deepika, 2 A. Sai Santhoshi , 3 D. Sowmya, 4 G.S.L.Sirsha 5 Mrs .D.Kiranmayi.

1Student, 2Student, 3Student, 4Student, 5Assistant Professor

1Vignan's Institute of Engineering for Women,

2Vignan's Institute of Engineering for Women,

3Vignan's Institute of Engineering for Women,

4Vignan's Institute of Engineering for Women,

5Vignan's Institute of Engineering for Women.

Abstract

The aim of this project is to demonstrate a digital watermarking scheme using visual cryptography for copyright protection of a digital image. A binary image, called watermark, is split into two shares via a 2-out-of-2 visual secret sharing scheme. Then, one of the shares called the master share is extracted from the host image using a fixed pseudo-random point, and the other share also known as ownership share, made by relating the master share and the watermark, is held by the owner which is also given to an authorized 3rd party copyright verifier. Based on the security property of visual cryptography, the two shares on their own cannot leak any information about the watermark. The experimental results show that even after the image was modified, the invisible watermark was successfully extracted from it.

Keywords: Digital Watermark, Visual Cryptography

INTRODUCTION

Compared to the old days, it has become super easy to make your information accessible to anyone around the world. That also means that it's trivial for someone to take your information, use it, and claim that it is his own.

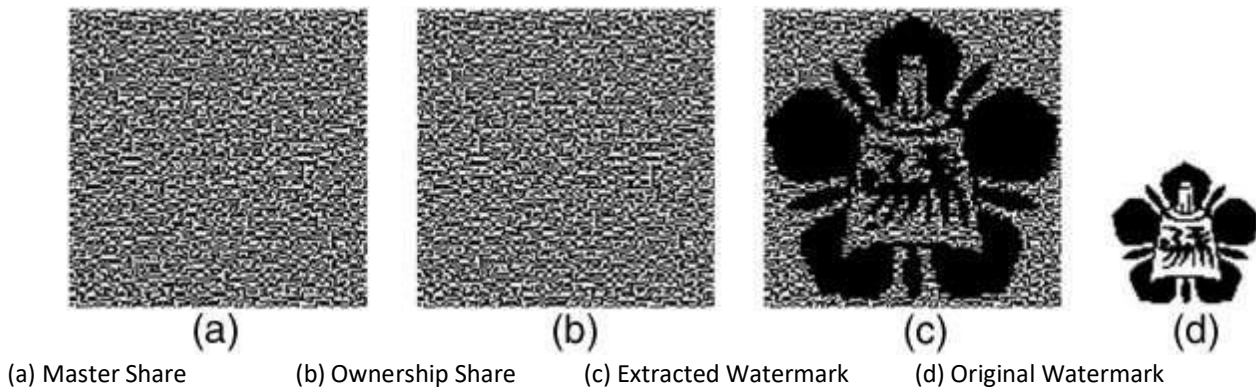
As an example, you may take a digital picture of a historical event that you may consider selling to Seattle Times. However, since you're greedy, a human being, and want to maximize the profit, you might've sent the photos to bunch of different companies to make them go on a bidding war. One individual that works at some company may then modify the image a little bit, claim that it's their original work, and essentially steal it. So what are you left with? Nothing, unfortunately, because you didn't know that you can protect your image even if it's in a digital format. How? You can embed extra information into digitized data to use as a protection—that is what digital watermarking is essentially.

Visible digital watermarking is something that is visible on the content. Invisible watermarking on the other hand can get a lot more interesting because the soon-to-be-criminal does not know that there is extra information in the data that he's trying to steal. Why do we care about invisible watermarking? That's because anything that one can "see" can be removed fairly easily—though it may require sophisticated software, it is definitely easier to remove something that one can see than removing something that one doesn't know what to remove. For example, if there's a logo at a right- bottom of a video, one can cover it up with another logo.

As we can see, there's clearly a reason to have invisible watermarking technology around. Compare to the visible watermarking that can be used for several purposes, invisible watermarking can do a lot more, enough to justify many different companies to put some researchers to work to build software that can do digital watermarking.

VISUAL CRYPTOGRAPHY

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. 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. Either transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. An example can be seen below.



Algorithm for Visual Cryptography

There is a simple algorithm for visual cryptography that creates 2 encrypted images from an original unencrypted image. The algorithm is as follows:

1. Create an image of random pixels the same size and shape as the original image.
Random1.
2. Create a second image whose pixels are the exclusive-or (XOR) of the first image and the original image.
Random2 = Random1 xor Original.
3. The two apparently random images can now be combined with XOR to re-create the original image.
Random1 xor Random2 = Original.

(2, 2) Visual Cryptography Scheme

A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary blocks of sub-pixels. While creating the shares, if the given pixel p in the original image is white, then the encoder randomly chooses one of the first two columns of Table. If the given pixel p is black, then the encoder randomly chooses one of the last two columns of Table. Each block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. Thus, no information is gained by looking at any group of pixels on a share.

Pixel	White □		Black ■	
	50%	50%	50%	50%
Share1	■□	□■	■□	□■
Share2	■□	□■	□■	■□
Stack Share1 & 2	■□	□■	■	■

THE METHODOLOGY ATTEMPTED

1. Ownership Share Generation

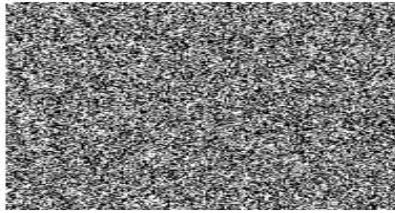
In this step, first, pseudo-random points are generated using a fixed key as a seed. Depending on the intensity of these points, a temporary master share is generated. Now the master share is *xored* with the original watermark image to get the ownership share.



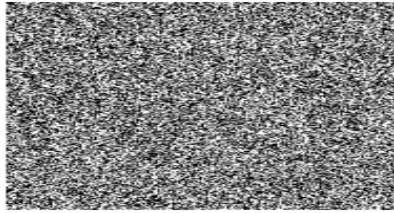
Original image



Original Watermark



Master share



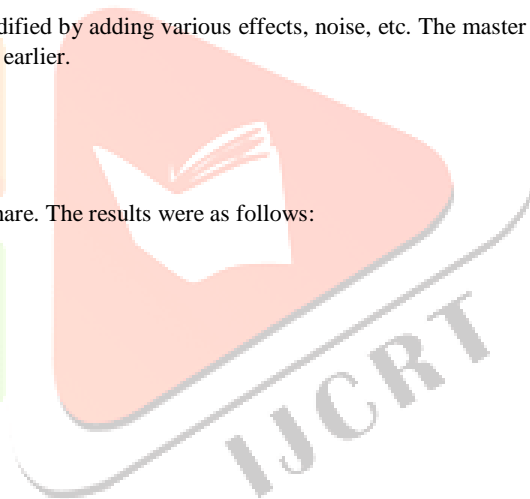
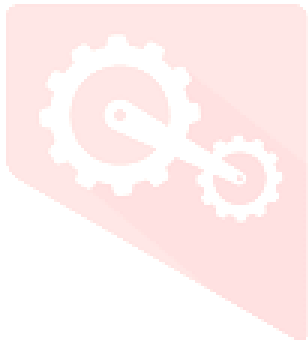
Ownership share








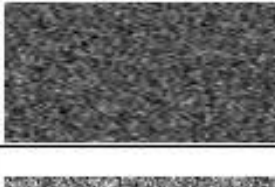



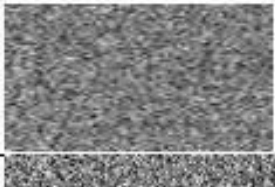


2. Master Share Generation from Modified Image

To emulate modified image, the original image was taken and modified by adding various effects, noise, etc. The master share from each one of them was then generated using the same points as taken earlier.

3. Watermark Extraction and Verification

The generated master shares were then *xored* with the ownership share. The results were as follows:



ATTACKS	MODIFIED IMAGES	GENERATED MASTER SHARES
MINOR CONTRAST ADJUSTED		
DECREASED BRIGHTNESS		
BLURRING		
SHARPENED		
SALT AND PEPPER NOISE		
FAKE VISIBLE COPYRIGHT		
DISTORTION		

COMPARATIVE STUDY

Visible digital watermarking is something that is visible on the content. For example, if there's a logo at a right bottom of an image, one can cover it up with another logo, where as one cannot do it if we use invisible watermarking.

A (k, n) visual cryptographic scheme encrypts a secret image into n share images (printed on transparencies) distributed among n participants. When any k participants stack their shares on an overhead projector (OR operation), the secret image can be visually discovered by a human visual system without the aid of computers (computation). But the monotone property of OR operation reduces the visual quality of reconstructed secret image for OR-based VCS. Generally all the conventional visual cryptography schemes (VCS) uses OR operation for stacking operations and so it is also called OR-based VCS. But it offers a poor visual quality image during decoding (stacking). Major advantage of XOR-based VCS (XVCS), is that since it uses XOR operation for decoding which results into exact recovery of the secret .

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

CONCLUSION

Template matching was used to match the extracted watermark with the original watermark and the results were noted. The results were positive despite modifications to the original image thus

No.	Type Of Modification to Image	Accuracy of Extracted Watermark
1	Minor Contrast Adjusted	88.14 %
2	Blurred Entire Image	85.58 %
3	Decreased Brightness	77.41 %
4	Salt Pepper Noise Added	87.06 %
5	Fake Visible Watermark Added	88.07 %
6	Distorted Entire Image	86.32 %

Visual cryptography offers perfect security for all the digitally transmitted secret images. 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 addition, VC-based watermarking may be used to robustify recognition of an extracted watermark from images which have been subjected to attacks.

FUTURE WORK

Our future work is to decrease the number of ownership share or reduce the size of ownership share.

In this XOR based cryptography is applied to both text and video. Some of the Data hiding algorithms can be applied to secure the image This paper has applications in military, bank etc the construction of the pixel is based on the random value.

The advantage of the proposed extraction scheme is that resolving the ownership can be done without the aid of the original image. However, the proposed scheme is not resistant to some attacks like rotations, cropping, scaling, and translations.

REFERENCES

1. Digital Watermarking Scheme with Visual Cryptography by Ching-Sheng Hsu and Shu-Fen Tu.
http://www.iaeng.org/publication/IMECS2008/IMECS2008_pp659-662.pdf
2. Wikipedia: Visual cryptography. https://en.wikipedia.org/wiki/Visual_cryptography#Cheating_the_.282.2CN.29_Visual_Secret_Sharing_Scheme
3. Visual Cryptography and it's applications by Jonathon Weir and WeiQi Yan.
<https://inspirit.net.in/books/security%20and%20hacking/Visual%20Cryptography%20&%20its%20applications.pdf>
A Visual Cryptography Based Digital Image Copyright.

