

Image Watermarking Using LSB and Visual Cryptography

Zinal M. Patel

M.E Student, Department of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology, Vasad, India

ABSTRACT: Image Watermarking is used for copyright protection, authentication and ownership of the intellectual property. Visual cryptography is technique in which secret data is decomposed into number of shares and distributed to participants, So that only participants can read that data. Image Visual Cryptography is used to keep the data private from unauthorized users. We are using both the approaches to protect data. We are combining Image Watermarking and Visual Cryptography techniques for detecting ownership of intellectual data. Watermark is broken down into two shares using visual cryptography. One of the shares is embedded into Original or Host image using LSB (Least Significant Bit) Watermarking technique. This will create watermarked image. This image is travelling over internet and if any unauthorized user will dispute that image or add noise to it then we can check our ownership by extracting one share from it. This extracted share is then xored with the second share which is kept private for handling such controversy.

KEYWORDS: LSB Watermarking, Visual Cryptography

I. INTRODUCTION

As technology increases, It is difficult to protect data and keep it private. Security in digital media has been a matter of serious concern. A Secure and an efficient communication of confidential and sensitive information is the initial concern in communication and network storage system. It is also important for any data not to be tamper. Now a day's much multimedia information is transmitted in large amount over internet. Especially while using images, secrecy is a major challenge. Because of this advancement in the network application securing image became a wide area to give attention .Visual cryptography and watermarking are used for securing images or text.

The General Framework of Watermarking is shown in below figure:

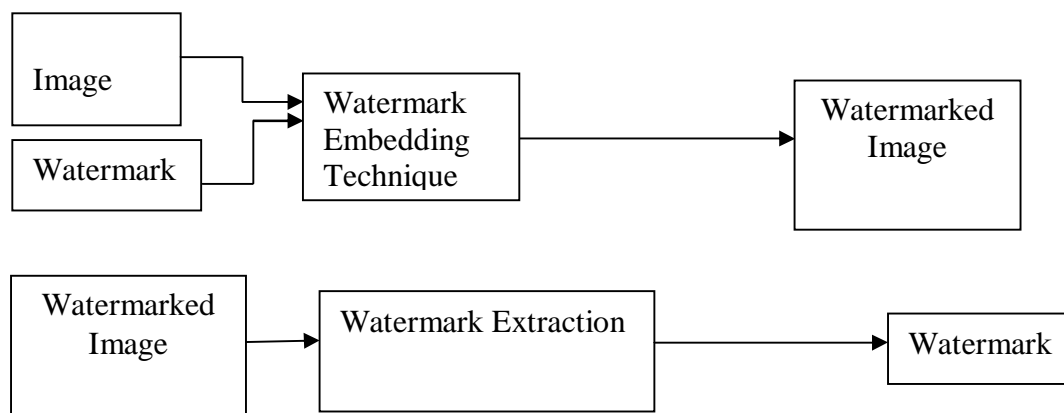


Fig. 1. General Framework of Watermarking

Visual Cryptography is a cryptographic technique which allows visual information (pictures, text etc) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. One of the best known



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994[1]. They demonstrated a visual secret sharing scheme, where an image was broken up 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. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

For the 2-out-of-2 VCS, the basis matrices, S^0 and S^1 are designed as follows[2]:

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

There are two collections of matrices, C_0 for encoding white pixels and C_1 for encoding black pixels. Let C_0 and C_1 be the following two collections of matrices[2]:

$$C_0 = \{ \pi(S^0) \}, C_1 = \{ \pi(S^1) \}$$

Where $\pi(S^0)$ and $\pi(S^1)$ represents the collection of all matrices obtained by permuting the columns of matrices S^0 and S^1 respectively[2].

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \text{ and } C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

To share a white pixel, the dealer randomly selects one of the matrices in C_0 , and to share a black pixel, the dealer randomly selects one of the matrices in C_1 .

II. RELATED WORK

Narasimha Swamy Gavini proposed Lossless Watermarking Technique for Copyright Protection of High Resolution Images in 2014 [3]. Yanyan Han and Wencai He proposed DWT-domain Dual Watermarking Algorithm of Color Image based on Visual Cryptography in 2013. Considering the combination of digital watermarking technique and visual cryptography, this paper proposes a new dual watermarking algorithm of color image. The first watermark is embedded into the high-frequency part of discrete wavelet transform (DWT). Using visual cryptography, we process the second watermark to generate two shares, then one of them is embedded into the low-frequency part of DWT and another is protected by the copyright [4]. Yanyan Han and Wencai He proposed A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform in 2014. Here, Watermark is processed to generate two shares based on visual cryptography. And one of the shares is embedded into a color image using DCT and another is protected by the copyright [5]. Yi-lin Bei, De-yun Yang, Ming-xia Lia and Li-li Zhu proposed A multi-channel Watermarking Scheme Based on HVS and DCT-DWT. The original image is transformed from RGB color spaces into the YCbCr color spaces in which watermark is embedding using DCT & DWT [6]. Seyed Mojtaba Mousavi & Alireza Naghsh proposed Watermarking Techniques used in Medical Images: a Survey in 2014. This paper aims to provide a useful survey on watermarking and offer a clear perspective for interested researchers by analysing the strengths and weaknesses of different existing methods [7].

III. PROPOSED ALGORITHM

Watermark Embedding Phase:

1. Generate two shares from watermark image using (2, 2) visual cryptography scheme. They are called Share1 and Share2. By overlapping them we can get original watermark.
2. Host image is color image. RGB that is RED, GREEN and BLUE component are taken from original image. Blue component of that image are used.
3. Using LSB watermarking technique, Share1 is embedded to the blue component of image. The other RED and GREEN component of the image are synthesized to get color image. This image is called watermarked image.
4. Share2 is kept private.

Watermark Extracting Phase:

1. Blue component are again taken from the watermarked image.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016





- Then using inverse operation of LSB watermarking technique, share1 is extracted from it.

IV. SIMULATION RESULTS

First of all, shares are generated from watermark using (2, 2) visual cryptography scheme. One of them is embedded using DCT to the blue component of host or original image. In this way watermarked image is generated. The share is extracted from watermarked image and xored with the remaining share. Finally watermark is generated. This is working of existing system.

In proposed system the shares are generated using (2, 2) visual cryptography scheme. One of them is embedded to blue component of host or original image using LSB algorithm. In that way watermarked image is generated. Share is retrieved from watermarked image using inverse LSB and the overlapped or xored with second share to get the original watermark. Experimental results of existing and proposed system are shown in below tables:

TABLE I. Experimental Result

Sr. No	Watermark	Original Image	Watermarked Image	Extracted Watermark	PSNR	MSE
1	fon			fon	7.0793	1.2739e+04
2	Copyright			Copyright	7.7029	1.1036e+04





Attacks are used to destroy the watermark from host or original image. Watermarking technique has the robustness against attacks. Attacks on image are categorized as below:

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

TABLE II.Experimental Result

Sr. No	Attack	Watermark	Proposed System Results	PSNR	MSE
1	Adding White Noise			5.7865	1.7156e+04
3	Croppi-ng			5.9131	1.6664e+04

V. CONCLUSION AND FUTURE WORK

The combination of both Watermarking and visual Cryptography techniques can provide some important solutions for tampering verification ownership of a given image. The characteristic of the visual Cryptography technique is used with watermarking to improve the security and robustness of the watermarks. We proposed LSB (Least Significant Bit) algorithm for watermarking and Visual Cryptography Scheme for share generation. It is robust against cropping and white noise (salt and paper noise) attacks.

REFERENCES

1. Moni Naor and Adi Shamir, "Visual Cryptography", Weizmann Institute, Rehovot 76100, Israel, 1998.
2. Chapter 2: REVIEW OF VISUAL CRYPTOGRAPHY SCHEMES, Department of Information Technology, Kannur University
3. Narasimha Swamy Gavini, Surekha Borra: Lossless Watermarking Technique for Copyright Protection of High Resolution Images, 2014 IEEE Region 10 Symposium.
4. Yanyan Han, Wencai He: DWT-domain Dual Watermarking Algorithm of Color Image based on Visual Cryptography, 2013 IEEE.
5. Yanyan Han, Wencai He: A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform, 2014 IEEE.
6. Yi-lin Bei, De-yun Yang, Ming-xia Lia and Li-li Zhu: A multi-channel Watermarking Scheme Based on HVS and DCT-DWT, 2011 IEEE.
7. Seyed Mojtaba Mousavi & Alireza Naghsh: Watermarking Techniques used in Medical Images: a Survey, Society for Imaging Informatics in Medicine 2014.
8. Han, Yanyan, Wencai He, Shuai Ji, and Qing Luo. "A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform", 2014 Ninth International Conference on P2P Parallel Grid Cloud and Internet Computing, 2014
9. Jonathan Weir, WeiQi Yan: Visual Cryptography and its applications bookboon.com
10. V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

BIOGRAPHY

Patel Zinal Manubhai is a Student in the Computer Engineering Department, Sardar Vallabhbai Patel Institute of Technology, Gujarat Technological University. She received Bachelor of Engineering (B.E) degree in 2013 from Engineering College Tuwa, Tuwa, Gujarat, India. Her research interests are security in digital media.