ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Survey on Image Watermarking and Visual Cryptography

Zinal M. Patel

M.E Student, Dept. of C.E., Sardar Vallabhbhai Patel Institute of Technology, Vasad, India

ABSTRACT: The development of information technology is increased now a day. Multimedia data requires security when it is used on internet. Image watermarking is used for hiding data as well as protecting that data from various attacks. 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. As E-commerce websites are revolved everywhere, copyright protection of intellectual property is prime concern. Using Image Watermarking techniques and Visual Cryptography, secrecy is maintained. This paper presents survey on various Image Watermarking techniques and different types of Visual Cryptography.

KEYWORDS: Image Watermarking, Visual Cryptography

I. Introduction

There is an increased development in the field of computer science and technology. As the large amount of multimedia data is travelling over the internet, Privacy and Protection of this data is needed. Various technologies are used to protect the multimedia data like watermarking and visual cryptography. Watermarking is used to protect content. It is used to hide the information. In social networking sites, when one can upload his/her photo then there is an option to download it. So anyone can use that photo. Photographers use watermarking for ownership of image. A watermark data is embedded in an image, video, audio to uniquely identify its owner and authorized user. Watermark data can be embedded at random locations within the content to make them difficult to detect and remove. Primary applications of watermarking are Copyright Protection, Content Authentication, Tamper Detection, Broadcast Monitoring, Forensics and Piracy Deterrence, Digital Fingerprinting etc.

II. Related work

A. *Classification of Watermarking*

1. Types of Information
    - Image
    - Audio
    - Video
    - Text

2. Working Domain
    - In spatial domain, the watermark data is directly embedded into the host information.
    - Wherein, frequency domain, the watermark data is embedded to the transformed version of host information.

3. Reversibility
    - In Reversible watermarking, after extracting watermark data, the original host information is also achieved.
    - In Non-reversible watermarking, after extracting watermark data, the original host information is not achieved.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

4. Human Perception

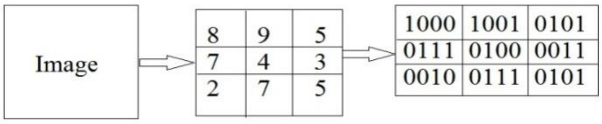
- Visible - Watermark data is visible to the human.
- Invisible - Watermark data is invisible to the human.
  - Fragile - This watermarking is sensitive to geometric attacks.
  - Semi fragile - watermarking is little bit more robust compared to fragile watermarking.
  - Robust - This watermarking is used for copyright protection.
  - Hybrid –This watermarking is combination of fragile and robust watermarking.
- Dual - Invisible watermark data is hidden behind visible watermark data

B. *Techniques of Image Watermarking*

Following are the five techniques of Image watermarking:

1. LSB(Least Significant Bits)

In this technique, the pixel values of image are converted into binary values. Pixels of Watermark are also converted to binary form. The LSB bits of each pixel are then replaced by watermark values. Following figure shows how it works:



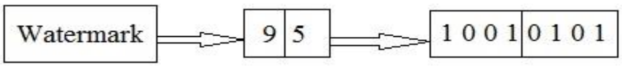
8	9	5
7	4	3
2	7	5

1000	1001	0101
0111	0100	0011
0010	0111	0101

Image Matrix of Pixel Binary Values
Values of Each Pixels

Fig. 1. Image pixels are converted into binary form

Image is made of pixel values. This pixel values are placed as matrix form. These pixel values are replaced with binary values as shown in fig. 1. Watermark image is also made of pixel values. These pixel values are replaced by binary values as shown in fig. 2.



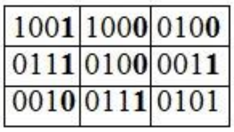
9	5

1 0 0 1	0 1 0 1

Watermark Pixel Values of Binary Values of
Watermark Each Pixel

Fig. 2. Watermark pixels are converted into binary form

LSB values of image are replaced by binary values of watermark as shown in fig. 3.



1001	1000	0100
0111	0100	0011
0010	0111	0101

Fig. 3. LSB bits are replaced by Watermark values

2. DCT(Discrete Cosine Transform)

DCT is used for compressing image. This will reduce the size. It is used to save memory requirement. In this technique, the image is broken down into blocks of N x N size. DCT is applied to each of this block. This will create DCT coefficient matrix of original image.

For example, $M = \begin{pmatrix} 50 & 72 \\ 65 & 78 \end{pmatrix}$

DCT has pixel values ranging from -128 to 127.Subtract 128 from all values of matrix M.
DCT of matrix B is calculated as below:

$$M = \begin{pmatrix} 50-128 & 72-128 \\ 65-128 & 78-128 \end{pmatrix}$$

$$= \begin{pmatrix} -78 & -56 \\ -63 & -50 \end{pmatrix}$$

Using below equations, DCT of matrix M is found[1] :

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) cos\left[\frac{(2x+1)i\pi}{2N}\right] cos\left[\frac{(2y+1)j\pi}{2N}\right] \qquad \text{eq. (1)}$$

$$T(i,j) = \left\{\begin{matrix} \frac{1}{\sqrt{2N}} & if\ i = 0 \\ \sqrt{\frac{2}{N}} \cos\left[\frac{(2j+1)i\pi}{2N}\right] & if\ i > 0 \end{matrix}\right\} \text{eq. (2)}$$

Here, N is the size of the block = 2
i= 0 to 1, j= 0 to 1, x= 0 to 1, y= 0 to 1
Using eq. (1) andeq. (2), We get the following matrix T :

$$T = \begin{pmatrix} 0.7071 & 1 \\ 0.7071 & -0.7071 \end{pmatrix}$$

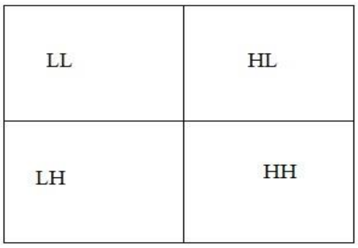
$$T' = \begin{pmatrix} 0.7071 & 0.7071 \\ 1 & -0.7071 \end{pmatrix}$$

$$TMT' = \begin{pmatrix} 0.7071 & 0.7071 \\ 0.7071 & -0.7071 \end{pmatrix} \begin{pmatrix} -78 & 56 \\ -63 & -50 \end{pmatrix} \begin{pmatrix} 0.7071 & 0.7071 \\ 1 & -0.7071 \end{pmatrix}$$

$$= \begin{pmatrix} -173.145 & -20.192 \\ -11.743 & -4.500 \end{pmatrix}$$

3. DWT(Discrete Wavelet Transform)

In this technique, Image is broken down into four bands LL (Low-Low), LH (Low-High), HL (High-Low) and HH (High-High). This is called first level of DWT. As bands increases, level of DWT increases.



LL	HL
LH	HH

Fig. 4. Bands of DWT

4. DFT(Discrete Fourier Transform)

In Mathematics, the DFT converts a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids, ordered by their frequencies, that has those same sample values. It can be said to convert the sampled function from its original domain to the frequency domain.

5. SVD(Singular Value Decomposition)

SVD uses one single matrix A which is decomposed into three matrix. The SVD is a factorization of a real Or complex matrix. It has many useful applications in signal processing and Statistics [2].Steps to calculate SVD of any matrix A are below :

$A= USV^T$

Where U and V is orthogonal matrix.

That means $U^TU = UU^T= I$ and $V^TV =VV^T= I$ (I is identity matrix.)

First find AA^T, and then calculate eigenvalue and eigenvector of AA^T.

Eigenvectors of AA^T constitute the columns of matrix U.

Now, Find A^TA , then Calculate eigenvalues and eigenvectors of A^TA

Eigenvectors of A^TA constitute the columns of matrix V.

V^T is transpose of matrix V·
Square roots of eigenvalues in diagonal way constitute the matrix S.

Finally, Multiplications of this three matrix U, S and V^T gives the singular values.

III. VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information like images to be encrypted in such a way that decryption is done by human eyes. This technique was first developed by Moni Naor and Adi Shamir in 1994.Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns. If the shares are XORed (Exclusive OR Operation) onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset [3].

Visual cryptography is used for key management, authentication, identification, data privacy, access control and remote electronic voting. Following are different types of visual cryptography:

1. Traditional Visual Cryptography

In traditional visual cryptography, Binary image is used as host image. Visual cryptography scheme is used to generate shares of host image. Shares are overlapped to construct the original host image. ‘1’ is used to represent black pixel and ‘0’ is used to represent white pixel. Each pixel of the host image is split onto black and white pixel. Here, Pixel is divided into of 2x2 schemes. That means white pixel is replaced by one of below probabilities:

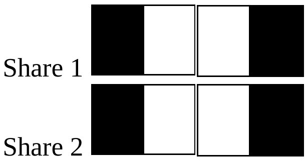


Fig. 5. Probabilities for White Pixel

Black pixel is replaced by one of below probabilities:

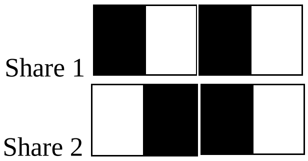


Fig. 6. Probabilities for Black Pixel

2. Halftone Visual Cryptography

In this Visual Cryptography, the host image is converted into halftone image. Two shares are generated from this halftone image. By overlapping two shares, we get the host image. The general printer, such as dot matrix printers, laser printers, and jet printers, can only control a single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the color tone of an image directly. As such, the way to represent the gray level of images is to use the density of printed dots; for example, the printed dots in the bright part of an image are sparse, and those in the dark part are dense [4]. The method that uses the density of the net dots to simulate the gray level is called “Halftone”[5].

3. Color Visual Cryptography

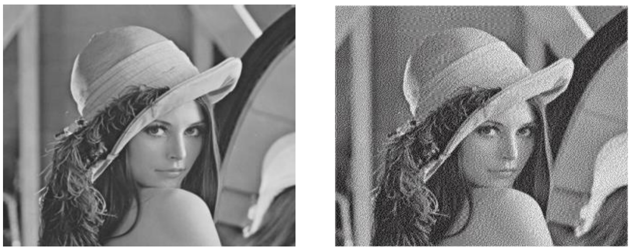
In this Visual Cryptography, The color image is converted to different color models like RGB, CMY, HSI, YIQ etc. In below figure, CMY color model is used. Now, these three images are half toned and then overlapping them we will get the original image.

4. Extended Visual Cryptography

In visual cryptography scheme (VCS), the image is encoded into number of shares. These shares are then superimposed on each other to get original image. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS) [6]. It means the shares are embedded into other meaningful images. So no one can have idea that it contains secrete inside it.

IV. RESULTS

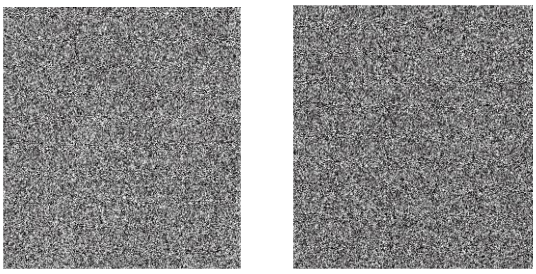
Halftone visual cryptography is performed on host image. The results of how it would be worked are explained below:



Host Image   Halftone Image

Fig. 7. Host Image and Halftone Image

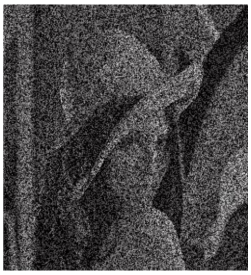
Above fig. 7 has two images. One is host image and other is halftone image of the host image.Now, This two shares are generated as share1 and share2 from this halftone image as shown in fig. 8.



Share1   Share2

Fig. 8. Shares generated from Halftone Image

Overlapping these two shares,we get the extracted halftone host image as shown in fig. 9.



Extracted Host Image

Fig. 9. Host Image generated from Overlapping shares

Original image is converted into CMY color model as shown in fig. 10. Then halftone image of these three images C, M and Y is generated. Now overlapping these three images, we get the original image. In this way, color visual cryptography is working.

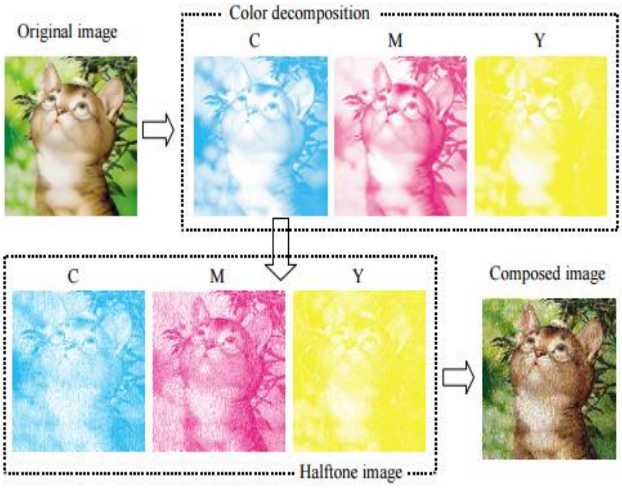


Fig. 10. Color Visual Cryptography [4]

Survey on different watermarking algorithm is done. From that we conclude their pros and cons as below:

TABLE I. Comparative Analysis of Watermarking Techniques

Sr. No	Domain	Method	Pros	Cons
1	Spatial	LSB	Easy to understand, Simple and less complex	Fragile to various geometric attacks
2	Transform	DCT	Fast and robust against JPEG compression	Blocking effect and Effect of picture cropping
3	Transform	DWT	Higher compression ratio and Higher flexibility	High cost, Produces blurring and ringing noise near edge regions in images, Longer compression time
4	Transform	DFT	Used to recover from geometric distortion	Output is always in complex value ,computational efficiency is

				poor
5	Transform	SVD	Change in singular values does not affect the quality of image; Singular values of an image have high stability, so they do not change after various attacks.	False Positive Rate Problem

V. Conclusion and Future Work

Image Watermarking is used to protect digital media on internet. In this paper, survey of different watermarking techniques LSB, DCT, DWT, DFT and SVD are analysed. The pros and cons of the watermarking techniques are listed in table. In this paper, Different types of Visual Cryptography are explained.

References

1. Ken Cabeen and Peter Gent," Image Compression and Discrete Cosine Transform", Math 45 College of the Redwoods.
2. http://web.mit.edu/be.400/www/SVD/Singular_Value_Decomposition.htm
3. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo "Halftone Visual Cryptography",IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST
4. Young-Chang Hou,"Visual cryptography for color images", Pattern Recognition 36 (2003) 1619 – 1629
5. C.A. Poynton, Frequently asked questions about color, http://www.inforamp.net/~poynton
6. Feng Liu and Chuankun Wu," Embedded Extended Visual Cryptography Schemes", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011
7. Mohanty SP, Ramakrishnan KR: A dual watermarking technique for images, in Proceedings of the 7th ACM International Multimedia. ACM Press, 1999, pp 49–51.
8. Seyed Mojtaba Mousavi & Alireza Naghsh &S. A. R. Abu-Bakar, "Watermarking Techniques used in Medical Images: a Survey",Society for Imaging Informatics in Medicine 2014
9. Moni Naor and Adi Shamir, "Visual Ctyptography",Weizmann Institute ,Rehovot 76100,Israel,1998.
10. PreetiParashar and Rajeev Kumar Singh, "A Survey: Digital Image Watermarking Techniques",1994.
11. 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 Manubhaiis a Student in the Computer Engineering Department, Sardar Vallabhbhai Patel Institute of Technology,Vasad,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.