Digital Watermarking Based on Visual Cryptography: A Survey

Sunesh¹, R. Rama Kishore²

¹MSIT, JANAKPURI, NEW DELHI, USICT, IPU, Dwarka, New Delhi
²suneshmlk@gmail.com

Abstract: In today's era, technology has made the transmission of digital content as child play as well as raises various copyright issues. Watermarking is one of the prominent solutions to online data vulnerability and copyright violations. However, maintaining equilibrium between robustness and imperceptibility at same time is concerned issue. So in such cases, digital watermarking based on visual cryptography (VC) is employed instead of watermarking. Digital watermarking using visual cryptography has been gaining immense importance where high protection of digital content is required. In this survey, various Visual Cryptography and watermarking techniques based on visual cryptography are discussed. However, main focus of this survey is on (2, 2) VC based watermarking in which two shares has been generated by using watermark and cover images.

Keywords: Watermarking, visual cryptography, watermark

1. INTRODUCTION

In last few decades, the proliferation of digital content over the internet has been increased. With this advancement, at one side transfer and processing of digital data has become faster and efficient whereas on other side unauthorized duplication and manipulation of digital multimedia (called copyright violations) has become serious problem. Because of these security concerns over copyright protection of digital content comes out as an emerging issue. Watermarking comes out as a raising solution which summates author information called watermark into multimedia data for purpose of copyright protection, image authentication, and copy protection. A watermark can be embedded at transform domain or spatial domain as reported in literature [1-5]. At transform domain, an image is represented in terms of frequencies i.e. image is segmented into multiple frequency bands. Watermarking at transform domain can be applied by using any of the transform like DCT, DWT, and DFT. Every transform represents image by different ways and has their own characteristics. To achieve the objective of copyright protection, it must interfere with mentioned conditions: namely Robustness, Imperceptibility, Security, Blindness and Unambiguity.

To maintain good image quality and robustness against attacks, some lossless watermarking approaches have been proposed. Visual cryptography (VC) is one of the lossless watermarking approaches used for achieving above said conditions of copyright protection. Visual cryptography proposed by Naor and Shamir in 1995 has been utilized in watermarking for information hiding into cover image [6-10].

Visual cryptography is a technique for information hiding into images in such a way that, it can be decrypted by human vision only when correct key is used [7, 11-13]. Visual cryptography represents secret image by several different shares. It is very difficult to get indication about secret message by individual share. When all shares of secret messages is stacked together only then secret message will be revealed [8]. This scheme does not require any computation for the reconstruction phase. Fundamental idea given by Naor and Shamir VC scheme is dividing secret image into two shares. Initially (2, 2) scheme is applied on binary images. In this each pixel of binary image is encoded into two shares s1 and s2. There is several cryptography techniques reported in literature [7, 9, 12-14] that uses VC schemes with two pixels or four pixels approaches. Some of the schemes that are presented in history are Joint Visual cryptography and watermarking technique reported by Ming et al. In this scheme, firstly noise employed into original image and then pair conjugates error diffusion performed for generation of two shares. Embedding of noise helps in diverting hacker’s attention from shares.

W.P. Fang reported a progressive viewing method for sharing of sensitive images Where each pixel was expanded into 2*2 block B(x, y) and then n transparencies are created. Han Yan-yan et al developed (2, 2) visual cryptography scheme based on watermarking as an extension of traditional cryptography. This proposed scheme is robust and imperceptible which can be applied on both gray and colour images.

Jithi et al reported a progressive visual cryptography with watermarking for meaningful shares. This generation of meaningful shares has achieved by combining watermarking with VC. This scheme uses unexpanded shares that resolves...
three main problem of VC i.e. pixel expansion, leak of secret information and bad quality of recovered image. In this technique, first secret image is divided into N shares then shares are superimposed with cover image to generate meaningful share. On other hand at decryption side, in first step original shares are extracted from meaningful share. Secret image is revealed gradually by superimposing more and more shares progressively.

Use of VC with watermarking makes extraction process simpler and also increases robustness and security. In this paper, newly emerging watermarking techniques based on visual cryptography (VC) are reviewed. Digital watermarking based on VC is classified into three different types: watermarking using (2, 2) VC, watermarking using (2, n) VC and watermarking using (k, n) VC. In this, the main focus is on watermarking based on (2, 2) visual cryptography.

2. RELATED WORK

Watermarking based on visual cryptography is an emerging scheme mainly used for achieving copyright of the owner. Various watermarking techniques are reported in literature review [6-8, 16-20]. When visual cryptography scheme is enforced with watermarking then watermark is inclined as input to visual cryptography. Numbers of shares are acquired by use of visual cryptography, one of these share enforced as input in embedding phase and whereas another share is given to certified authority whose intervention is requested (if dispute occurs).

Watermark pattern may or may not be physically inserted into cover image. So watermarking schemes based on VC lies into two categories. In first category, physically embedding of watermark takes place and second is Concealing scheme. In concealing scheme original image is not altered. Watermarking based on VC can be classified in three ways which are as follows:

1. Digital watermarking based on (2, 2) VC
2. Digital watermarking based on (2, n) VC
3. Digital watermarking based on (k, n) VC

2.1 WATERMARKING WITH (2, 2) VISUAL CRYPTOGRAPHY SCHEME

Many researchers have carried out research in the field of watermarking based on (2, 2) VC. Initially, Young et al presented an asymmetric watermarking scheme based on (2, 2) visual cryptography. For achieving copyright protection objectives, Digital watermarking utilizes (2, 2) Visual cryptography. Digital watermarking based on (2, 2) consists of two phases: embedding and extraction phase explained in Fig.1 and fig.2.

In this watermarking method, (2, 2) VC scheme is applied on watermark which produces two random noise looking share. One share is registered with trusted authority (TA) who can resolve dispute, in case if occurs. Other share is then inserted into host data. The way of insertion into host data may vary. Extraction process is shown in fig 2. Watermark can be revealed only when both random looking shares are stacked together. In this survey paper, we will classify watermarking into two broad categories mentioned below:

1. (2,2)Visual cryptography based approach at spatial domain
2. (2,2)Visual cryptography based approach at Transform domain.

In spatial domain watermarking approaches, watermark is directly embedded by modifying the spatial characteristics such as pixel values. Initially watermarking approaches utilizes (2, 2) VC scheme for copyright protection of images by using scheme proposed by Naor and Shamir in 1995. In literature, first time Young et al reported an asymmetric watermarking scheme based on visual cryptography where embedding took place into two steps. At first step, watermark is divided into two shares in which one share acts as a cipher text and other share called as secret key is used for extracting watermark from watermarked data. These shares appear like random noise. In second step one share of watermark called cipher embedded into host data and resultant produced is called stego image. This stego image may be transmitted over transmission media. For extracting watermark from stego image, second share called secret key superimposed onto stego image then watermark will be revealed. If any of these two shares is modified then watermark cannot be revealed.

Tzung et al reported an owner- Customer copyright protection mechanism using a watermarking scheme and a watermarking protocol. It enables owner to prove his copyright by using copyright share and customer to show his legal ownership by using ownership share. In this, author developed watermarking scheme based on visual cryptography and watermarking protocol using asymmetric
cryptography. Combining VC with watermarking provides benefits to security and reliability of copyright.

Hao et al developed a multiple watermarking by using non expansion VC for gray level images. Use of non-expansion makes shares equal to secret image and requires less storage space for shares. This method embeds two watermarks. Insertion of first watermark took places during error diffusion half toning process and second watermark inserted into image during halftone image encryption process. For extracting watermark, ex-or operation is performed.

Aditya Vashistha et al developed a robust video watermarking based on VC and scene average image for watermarking video content. Firstly abrupt scene change was detected. Scene change detection is calculated using segmentation method. Segmentation method based on color difference between consecutive frames of video and starts frame position of new scene is checked by peak. Secondly scene start point information vector is used to find average scene frame. Lastly to find verification Information vector for each averaged scene frame and then scene image converted into gray scale image for computation of verification vector.

Number of VI = Number of scene = Number of frame averaged scene

Adel reported their work on a visual cryptography based digital image copyright protection which utilizes relationship between randomly selected pixels and their eight neighboring pixels of watermark pattern P(x,y) that results verification information. Security of this approach depends on this relationship.

B. Surekha et al presented security analysis of a novel copy right protection scheme using visual cryptography proposed by A. nag is a concealing scheme which does not perceptually degrade quality of image. This scheme based on spatial domain where MSB bits of cover image utilizes as features and (2, 2) VC code book with pixel expansion as four for constructing the shares. In their analysis, it is shown that scheme contains of weak features and poor design those results high ambiguity while verification of ownership. Approach is simple, insecure and resist to common processing attack.

2.1.2 WATERMARKING BASED ON VISUAL CRYPTOGRAPHY AT TRANSFORM DOMAIN

In transform domain watermarking techniques, first transformation techniques are applied on the image and watermark is then embedded by modifying transformation co-efficient. Transform domain techniques are more robust comparison to spatial domain techniques.

Der-Chyuan Lou et al developed a copyright protection scheme for images at transform domain using (2, 2) VC. In this approach instead of embedding watermark into cover image, two shares of both watermark and cover image is generated called public and secret share. This secret image is produced by using code book (described in this paper) and feature value. Feature value is calculated from cover image by performing under mentioned three steps:

1. Decomposing cover image into ten sub bands by 3-level DWT and then extract low sub bands (L) and middle sub bands (M).
2. Then calculate new co-efficient (L’ ) from low sub band (L).
3. After preforming above two steps difference between low sub bands and new co-efficient is taken

\[ F(I, J) = \begin{cases} 1 & \text{if } L(I, J) > L'(I, J) \text{ and } 0 \text{ if } L(I, J) \leq L'(I, J) \end{cases} \]

Watermarking extraction is achieved in two phases. Firstly feature value has been extracted from suspected image and this feature value is utilized to generate public image depending on code book of VC. In Second step, by performing Ex-OR operation between secret image and public image watermark can be obtained. This scheme is robust against JPEG lossy compression, scaling, noise adding, blurring, sharpening, mixing and special attacks because characteristics of DWT and VC.

Tzung-her chen et al reported security analyses of copyright protection scheme presented by Der-Chyun Lou et al(4). From theoretical analyses and experimental results it was found that approach highly robust but sustains with false positive error i.e owner itself can extract watermark from alterate image by utilizing same secret key.

Gwo-chin Tai et al outlines a public digital watermarking based on (2, 2) visual cryptography scheme for still images. In this, Wavelet Packet Transform has been employed on the original image. After that, public and private share image are generated by applying (2, 2) VC approach on secret image and features of host image that provides security and robustness. Public share is used as watermark and protected with error correcting code which increases reliability of watermark. Private share is required for revealing the original watermark.

Ming-shi Wang et al reported a hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. First,two level DWT and SVD is applied on host image and extracts features vector values that helps in achieving robustness of the scheme. After that K-means clustering applied on these extracted features values and master share is generated by utilizing clustering result. By employing this master share with secret image, ownership share is constructed. For construction for ownership share (2,2)VC is used that helps in achieving copyright protection.

D.Mathivadhani et al outlines an hybrid approach that combines digital watermarking with Visual cryptography scheme. This model is robust against various attacks as well
as it also maintains visual quality of cover image and secret message. Secret image and iris image to be used as watermark. In first both secret message and iris image has been processed by utilizing different methods. Processing(encoding) of secret message take place by using Visual cryptography(VC) method. Secret message is divided into two shares called S1 and S2 by applying VC and then compression performed on same. For hiding iris image into cover image, feature of iris image is extracted called iris code. Iris image is limited 256* 256 gray scale image. Iris code is to be used for authentication purpose.In second phase cover image is decomposed into sub bands using 2-D haar wavelet transform then embedding of watermark bits take place at LSB. Embedding starts with compressed bits followed by iris code. LSB selects only one of three colors at each pixels of cover image.Extraction process is just reverse of embedding process. Above said system resists JPEG, Gaussian noise, median filter, blurring, gamma, cropping, resizing, rotation and affine transform attacks.

Sanjay Rawat et al proposed a robust watermarking scheme based on Fractional Fourier Transform FFT and VC. Security and robustness is achieved in this scheme by employing properties of FFT, SVD and VC. In this, features of host image were extracted by using FFT and SVD that provides security and robustness. FFT is very sensitive to its transform order. No one can extract watermarking without knowing correct transform order which ensures security of scheme. These extracted features are used for generation master share and ownership share by applying visual cryptography. Watermark is revealed by stacking shares together because of (2, 2) VC.

Th. Rupachandra singh et al presented a novel approach named robust video watermarking scheme based on visual cryptography which uses single invisible watermark. In this watermark is divided into equal size sub watermark and no. of sub watermark is equal to number of scene present in video. In their approach, authors achieved embedding of watermark into three steps; video preprocess, Owner share generation. In video preprocess phase, first scene change detection performed by applying histogram difference method at 2-level DWT. Insertion of watermark made at LL band and then owner share and identification share is generated by using frame mean and global mean that helps in achieving robustness. It was shown by experimental results this approach is robust against frame dropping, averaging, swapping, image processing attacks and statistical analysis.

Meryerm et al outlines a blind, invisible and robust watermarking technique using visual cryptography. In this, DT-CWT transform applied on image that provides results in form of binary matrix B (based on LL sub band features). Binary matrix B is used for generating shares from watermark by applying Pixel expansion (2, 2) visual cryptography that makes scheme robust against attacks. For extracting watermark public and private share are stacked together. Extraction process is followed by reduction process that resolves pixel expansion by coding pair of pixels.

Yanyanhan etal developed DWT-domain dual domain watermarking algorithm that increases robustness and security. In this, for embedding watermark firstly blue component is separated then divided into two resolution level by using 1-level DWT. Both watermark are processed first and then inserted into host data. First watermark W1 is processed by applying Arnold transform which results scrambled watermark output. This resultant watermark embedded at high frequency part. Second watermark is processed by applying visual cryptography in which two shares are generated which makes watermark more secure and robust. One of share is inserted onto low frequency part of DWT that increases robustness of a watermark.

Geum-dal Park et al proposed Lossless codebook-based digital watermarking scheme with authentication. This scheme solves ambiguity problem of Xing et al scheme. Ambiguity problem was solved by use of lossless codebook that uses AND and OR Boolean operations. In this scheme, 3-level DWT applied on cover image and extracts LL sub-band features. Then these extracted features, codebook and watermark are utilized for generating share. Lossless codebook brings non expansion of watermarked image.

Meryerm et al reported a Medical image watermarking scheme based on visual cryptography and dual tree – Complex wavelet transform (DT-CWT for high protection of medical image content. This algorithm consists of three phases: watermark concealing, watermark extraction, watermark reduction. Watermark concealing and extraction follows same steps for generation for private and secret share respectively. Reduction process removes redundancy caused by VC scheme which improves visual quality of extracted watermark. This method is reliable and robust against various image processing attacks shown in experimental results. This allows insertion of watermark without altering host data. However, this type of methods helps in protecting highly sensitive images.

2.2 WATERMARKING WITH (2, N) VISUAL CRYPTOGRAPHY SCHEME

Embedding phase of watermarking scheme with (2, n) visual cryptography scheme are same as watermarking with (2,2) visual cryptography with one difference. The difference is type of visual cryptography approach applied on watermark. Embedding process of watermarking with (2, n) VC scheme explained in fig.3. In this multiple (n) shares are generated by applying (2, n) VC on watermark. Only one share will be used by owner while other shares are submitted to different trusted authorities (TA) for intervention if required.
Extraction process is same as described in previous method called watermarking with (2, 2) VC. In case of dispute, sometimes TA may be unreachable in (2, 2) VC due to some reasons like corruption etc. This disadvantage of watermarking with (2, 2) VC is overcomes by (2, n) method of watermarking. In this n shares are deposited to various trusted authorities that solves problem of TA failure. The steps of extraction phase are represented by fig.7. In 2014, Stelvio also outlines watermarking based on (2, n) visual cryptography scheme where numbers of shares are generated.

Watermarking with (k, n) VC approach is further extension of previous two schemes as explained in Section 2.1, 2.2. Watermarking based on (k, n) is reported by Stevlio et al. In this watermarking technique, (K, n) visual cryptography can be utilized for insertion of watermark. Embedding and extraction process of this approach remains same as explained above. This watermarking technique uses (k, n) visual cryptography, instead of (2, 2) VC or (2, n) VC. When (k, n) VC is applied on watermark data at embedding phase then watermark data is subdivided into n different shares and for extracting watermark only k shares out of n shares are required. Watermarking based on (k, n) visual cryptography has been outlined by Stelvio in 2014.

3. ANALYSIS AND DISCUSSIONS

Robustness, Imperceptibility, Security, Blindness and Unambiguity are important issues in the watermarking field for measuring performance of the scheme. Performance of a watermarking approach based on VC is measured mainly in terms of Peak Signal to Noise Ratio PSNR and Normalized co-relation NC [22, 25-26, 30]. Watermarking scheme are checked against various attacks like JPEG compression, cropping, adding noise, resizing, blurring, sharpening, contrast adjustment, gamma correction, histogram equalization, rotation and median filtering and values of PSNR and NC are calculated.

PSNR is used to measure the quality of image. Basically, it is used to evaluate visual quality between watermarked image and original image. Higher the PSNR, Lesser the distortion will be in the image. Work discussed above [6, 10-11, 18, 22, 25-27, 29-31] are used PSNR for evaluating the performance against various attacks. The number of attacks is decided by the author itself and also based on the basis of the type of application.

Normalized co-relation NC is used to measure similarity between original and extracted watermark. It also determines whether watermark is exists in image or not depending upon the value of co-relation. If correlation is larger than predefined threshold then it assumed watermark exists. Already discussed work [10, 24-30] uses NC to measure the performance of the watermarking schemes based on VC. The similarity can be defined on the basis of the results of NC.

Geum-dal Park et al defined accuracy Ratio AR as the ratio of number of common bits in original and extracted watermark. If AR value is nearer to 1 then it reflects extracted watermark is similar to original watermark. Work [6, 31] discussed above have used AR for evaluating the performance.

In a nutshell, all of the above discussed NC, PSNR, AR results are used to decide whether the scheme is robust and secure or not.

4. CONCLUSIONS

In this paper, we have mainly discussed various visual cryptography techniques, watermarking techniques based on visual cryptography. Some of our finding from this survey given below:

1. Security of a robust approach is depends on the way the code blocks are chosen for substitution. Because different cover images may generate similar share for same watermark.

2. False positive rate should be low for achieving accurate results in case of ownership conflicts. False positive rate represents less ambiguity in revealing the right owner.

3. Visual quality of image can be also maintained by the use of invariant VC. Invariant VC does not involve pixel expansion.

4. Mainly, watermarking based on VC has been used for purpose of copy right protection that helps in resolving ownership conflicts. Because one share of watermark is submitted to TA that helps in resolving ownership conflicts.
5. Use of visual cryptography in watermarking makes extraction process easy as compared to basic watermarking scheme because extraction process involves simply stacking of shares or ex-or operation.

6. Watermarking based on VC can conceal watermark without modifying cover image. Concealing of watermark is performed by simply extracting features of cover image and watermark.

7. To the best of my knowledge, (2, 2) VC is used in watermarking.

8. Our analysis is that use of visual cryptography in watermarking constructs watermark more secure and robust against the attacks in comparison to other watermarking approaches (without use of visual cryptography). Security characteristics of VC makes watermark more robust and secure.

5. FUTURE SCOPE

The work presented in this paper may be expanded into given below directions:

1) By combining watermarking with (2,n) visual cryptography

2) By employing (k, n) Visual cryptography in watermarking

Combining watermarking with (2, n) and (k, n) visual cryptography will increases security and robustness of watermark.

REFERENCES


