Optimal Number of Shares For Digital Watermarking Scheme Using Visual Cryptography

Jitendra Saturwar ¹, Dr. D.N.Chaudhari²

¹Department of Computer Sci. & Engg, Jawaharlal Darda Institute of Engg. & Technology, Yavatmal, India
²Department of Computer Sci. & Engg, Jawaharlal Darda Institute of Engg. & Technology, Yavatmal, India

ABSTRACT

With the growth of digital media, it is becoming more prevalent to find a method to protect the security of that media. An effective method for securely transmitting images is found in the field of Visual Cryptography. Digital music downloads, video-on-demand, and multimedia social networks pose new challenges to the design of content protection measures aimed at preventing copyright violations. Digital watermarking has been proposed as a possible brick of such protection systems. However, application of watermarking for multimedia content protection in realistic scenarios poses several security issues.

The adoption of efficient methods for watermark embedding or detection on data that have been secured in some way, which we name in short secure watermarking, provides an elegant way to solve the security concerns of applications. A digital watermarking technique is used to generate meaningful shares. The secret image shares are watermarked with different cover images and are transmitted. At the receiving side the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively. Digital watermarking using visual cryptography provides improved security for encrypting secret images.

Keywords — Watermarking, Visual cryptography, Image copyright, Cryptography

I. INTRODUCTION

A digital watermark provides a communication channel multiplexed into the original content through which it is possible to transmit some application-dependent information; in forensic tracing, a watermark can be used to embed a unique code, as a fingerprint, into each copy of the content to be distributed, linking the copy either to a particular user or to a specific device. When unauthorized published content is found, the fingerprint allows to trace the user who has redistributed the content [4], [24]. The adoption of digital watermarking techniques for multimedia content protection in realistic scenarios raises a set of important issues. One is represented by a possible malicious incrimination of an honest buyer (known in the literature as customer’s rights problem): when the watermark is embedded at the distribution server, a customer whose watermark has been found on unauthorized copies can claim that he/she has been framed by a malicious seller who inserted his/her identity as watermark in an arbitrary object.

Also, a secret key is given to embed “watermark pattern” and to retrieve it as well. Figure 1 gives summarize of standard watermarking embedding scheme. Basically, if the owner wants to protect his/her image, the owner of an image has to register the image with the copyright office by sending a copy to them. The copyright office archives the image, together with information about the rightful owner. When dispute occurs, the real owner contacts the copyright office to obtain proof that he is the rightful owner. If he did not register the image, then he should at least be able to show the film negative. However, with the rapid acceptance of digital photography, there might never have been a negative. Theoretically, it is possible for the owner to use a watermark embedded in the image to prove that he/she owns it.

A typical image watermarking algorithm must satisfy the following two properties: transparency and robustness. Transparency means that the embedded watermark pattern does not visually spoil the original image fidelity and
should be invisible. Robustness means the watermark pattern is not easy to detect and remove illegally. Moreover, any modifications of the image values have to be invisible, and the watermark method has to be robust or fragile in order to provide protection against attackers.

\[ \text{Watermark} \ W \rightarrow \text{data} \ 1 \rightarrow \text{embedding system} \rightarrow \text{Watermarked data} \ 1' \]

\[ \text{Secret key} \ K \rightarrow \text{data} \ 1 \rightarrow \text{embedding system} \rightarrow \text{Watermarked data} \ 1' \]

\textbf{Figure 1. Watermarking embedding scheme.}

\section{Literature Review}

Harsh K Verma et al. [26] uses a watermarking method to generate meaningful shares. In their method firstly, an image is decomposed into its bit plane images that generate a binary image at each bit plane. Secondly, the traditional binary secret sharing scheme is used to get the sharing images. Finally, a proposed watermarking technique is used to generate meaningful shares. To decrypt hidden secret image, extract the shares from the cover image and decompose each share into bit planes and then secret grayscale image is reconstructed. This scheme provides a more efficient way to hide images in different meaningful shares. Furthermore, the size of the hidden secret can be recovered by inspecting the blocks in the shares.

B. Surekha [3] suggested The concept of Visual Secret Sharing (VSS) is used to hide a digital watermark into Discrete Wavelet Transform of a host image. The features of the image are used to split the watermark into two random binary images called shares. One share is generated during watermark embedding phase and is kept secret with an arbitrator. The other share is extracted from the controversial image during watermark extraction phase. Both the shares are combined to extract the original watermark.

Hui-Wen Liao [4] suggested a multiple watermarking scheme for color images by using YCbCr color model, visual cryptography, histogram modification, integer wavelet transform, and the wavelet tree. Under this scheme, all owners will have dual watermark authentication, and the number of ownerships can be increased. Applying the proposed four points distinguishing law, the owner’s dual watermark can be extracted more imperceptibly. Usually, for multiple watermarking, the more embedding watermark will lead to less quality of watermarked image; however, in proposed procedure, the increased number of owners does not affect the quality of the watermarked image and the watermarks after extraction.

Adel Hammad Abusitta [1], proposed digital image copyright protection method using watermarking technology. The method does not require that the water-mark pattern to be embedded in to the original digital image. Instead, Verification information is generated which will be used to verify the ownership of the image. This leaves the marked image equal to the original image.

Advantage of this method is that a water-mark pattern can be retrieved easily from marked image even the image is attacked by major changes in pixels bits.

Shyamalendu Kandar et al. [5] proposes a Visual Cryptographic Scheme for color images where the divided shares are enveloped in other images using invisible digital watermarking. The shares are generated using Random Number.

B. Surekha et al. [6] also proposed a spatial domain digital image copyright protection scheme based on Visual Cryptography (VC) and Spatial Correlation of Colors (SCC) is proposed. A binary feature matrix, extracted from the spatial correlation of host image, is used to split the watermark into two noisy binary images called shares. One of them is generated during watermark embedding phase and is registered with a trusted third party. The other is extracted during watermark extraction phase. Both these shares are combined to recover hidden watermark.

Pradosh Bandyopadhyay et al. [7] framework is able to embed the color watermark images to color host images and perceptually the watermark is not visible in the watermarked image. We've used blind method for
watermark extraction. With addition to that we also ensure that the extracted watermark remains intact. Security issue is assured with a secret key and a hash function.

Saurabh Maheshwari et al.[8] proposed randomized threshold based visual cryptography scheme is used. Each of the shares generated is embedded into different block through different strategy. The transformations are applied depending upon the high and low frequency regions of the image after performing statistical analysis. The watermark embedding is done using three frequency transforms, DCT, DWT and DFT simultaneously in different blocks of the image to hide the information as to which transform is used in the block leading to security of watermark. The number of permutations to determine exact watermark locations has been derived mathematically.

Li Lianhuan et al. [9], proposes an adaptive image tamper positioning, detection and recovery fragile watermarking algorithms. Using k-means clustering algorithm and image spatial visual features associated with the establishment of mechanisms to block the image, digital image to achieve a return to the spatial domain fragile watermarking scheme, and the use of encryption technology to enhance the security of watermarking algorithm.

Oclay Duman et al. [10] proposed a binary image is utilized as a watermark which is embedded using the Discrete Wavelet Transform (DWT) and the Fractional Fourier Transform (FrFT). Use of DWT domain to embed the watermark into the original image in such a way that it is imperceptible by the human visual system. The FrFT orders are used as the encryption keys that allow the watermarking method to be more robust against various attacks. It is also shown that the watermark can be extracted from the watermarked image without needing the knowledge of the original image.

HAN Yan-yan [11] et al. Proposed a visual cryptography scheme with meaningful shares. Compared to the previous schemes proposed in the literatures, the scheme does not change the original pixel expansion, and not only applies for black and white binary images, but also for any gray and color images. Meanwhile, the embedded image in a meaningful share is robust. Before and after being extracted the image's quality did not change significantly.

Ching-ling wan et al. [12] proposed two image secret sharing schemes. The first scheme uses two share images to hiding three secret information images, while second scheme uses three share images to hiding four secret information images. By using rotating image and matching block method, the second scheme increase more hiding secret information images.

Young-Chang Hou et al. [13] Proposed a method does not need to alter the original image and can identify the ownership without restoring to the original image. Besides, our method allows multiple watermarks to be registered for a single host image without causing any damage to other hidden watermarks.

Ching-Sheng Hsu [14] suggested a method in which image is split into two shares via a 2-out-of-2 visual secret sharing scheme. Then, one of the shares is embedded into the host image, and the other is held by the owner. When proving the ownership, the owner has to extract the embedded share and recover the watermark with his/her own share. Based on the security property of visual cryptography, our scheme can make sure that the two shares cannot leak any information about the watermark.

III. METHODOLOGY/MATERIALS AND METHODS

A. Existing Technologies And Methods

Various methods for Digital Watermarking using Visual cryptography are suggested as given below:

- Random selection of pixel for deciding master share for visual cryptography by Young-Chang Hou et al.
- Multiple Secret Sharing Method by Ching-Ling Wang et al.
- Watermarking based visual cryptography with Meaningful Shares by HAN Yan-yan et al.
• Wavelet Domain watermark embedding and extraction using FFT proposed by Olcay Duman et al.
• Digital watermarking using DWT, SLSB and VC by Mrs. D. Mathivadhani et al.
• A Self-adaptive Blind Detection Color Watermarking Algorithm Based on Wavelet Contrast by Liu Dan.

B. Proposed Method

![Diagram showing visual cryptography process]

**Figure 2: visual cryptography using visual cryptography Proposed by Mustafa Ulutas (27)**

C. Methodology

In visual secret-sharing schemes for multiple secrets, each share is a form of random distributed black and white pixels (is indistinguishable from random noise). The inconvenience of these schemes is that they use meaningless shares to hide the secrets. A novel (2, 2) visual secret-sharing scheme with meaningful shares is proposed in this section.

Proposed method takes two secret and two cover images as shown in Figure 2. Cover images are used for construction of the meaningful shares. Two secret images are reconstructed by using these two meaningful shares. First share is constructed by using the two secret images and two cover images while second share is constituted by using the two secret images and second cover image.

During the decoding process, the first secret image becomes visible by just stacking the two shares. The second secret is revealed, after rotating the first share by $\theta$ degrees and stacking it with the second share. Proposed algorithm constructs the first share in a fully random manner different from Wu and Chen’s algorithm. Therefore, pixel values (black or white) of the cover images can be used for construction of the corresponding extended blocks in meaningful shares. If pixel value in cover image is black at a certain position, the $2 \times 2$ extended block of a share at that position should have one white and three black pixels. It means that the extended block appears like black as in cover image. If the pixel value is white in cover image, extended block at that position in a share has two white and two black pixels that appear white. Pattern selection process in an extended block will be explained in detail below. When two shares are stacked together, if all of the four subpixels in the $2 \times 2$ extended block are black, this block represents a black pixel in the secret image. If one white pixel exists in the extended block, this extended block would represent a white pixel. Hiding two secret images into two covers by the proposed scheme is more efficient than concatenation of two secret images into a single and larger image and then sharing it. Let secret images be of size $N \times N$. Concatenation of these images will result in an $N \times 2N$ image.

The size of resulting shares would be $2N \times 4N$ if Shamir’s visual secret-sharing approach is used. However, the proposed method generates shares of size $2N \times 2N$ with the same hiding capacity. Thus, the proposed method is preferable in terms of storage capacity and bandwidth requirements.

To increase the image security this research will employ the advantages of the VSS scheme to design the proposed technique in embedding the watermark into the image signal and reserve the secret watermark in the copyright holder.

D. Proposed System and implication

IJRISE | www.ijrise.org | editor@ijrise.org [57-63]
This research has chosen to use the Digital watermarking Technique with visual cryptography for encryption to get the following advantages:

1. **Transparency**: The embedded watermark pattern does not visually spoil the original image fidelity and should be perceptually invisible. Meaningful share images can avoid the aware of active attackers.
2. **Pixel expansion unchanged**: Compared to the previous schemes proposed in the literatures, the scheme does not change the original pixel expansion.
3. **Robustness**: The watermark pattern is hard to detect and remove in an illegal way.
4. **Portability**: The scheme not only applies for black and white binary images, but also for any gray and color images.
5. **Feasibility**: What this research chose is a class of watermarking, so the scheme is easy to implement and highly feasible.

**CONCLUSION**

Visual secret sharing scheme is one of the secret sharing scheme in which secret information is an image which is a collection of black and white pixels. Progressive visual cryptography can be utilized to recover the secret image gradually by superimposing more and more shares. Various methods in the field of visual cryptography and progressive visual cryptography have been discussed. Most of the method was based on pixel expansion which caused wastage of storage area. Some others have security problems.

There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. In the existing VC schemes no security is provided to the secret shares and adversaries can alter its bit sequences to create fake shares. And in proposed scheme, the vulnerability of these binary secret shares is overcome by hiding them invisibly into some host images. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because of watermark extraction technique.

**REFERENCES**


Digital Watermarking and Information Hiding Using Wavelets, SLSB

Enhancement of security in Visual Cryptography

The Image Watermarking Technique Using Visual Secret Sharing

NoMark: A Novel Method for Copyright Protection of Digital Videos Without Embedding Data


Liu Dan “A Self-adaptive Blind Detection Color Watermarking Algorithm Based on Wavelet Contrast” 2012 International Conference on Computer Science and Information Processing (CSIP), 978-1-4673-1411-4/12 ©2012 IEEE(pg no.1411-1413)


Chunhua Dong”A DWT-DCT Based Robust Multiple Watermarks for Medical Image”, 978-1-4577-0911-1/12 ©2012 IEEE