IRA-International Journal of Technology & Engineering ISSN 2455-4480
Proceedings of the
International Conference on Science & Engineering for Sustainable Development (2017)
Pg. no.93-100
Published by: Institute of Research Advances
https://research-advances.org/index.php/IRAJTE

Performance Evaluation of watermarking Schemes to Decide Meaningful Number of Shares

Jitendra Saturwar*[1], D.N.Chaudhari[2]
[1,2] Department of Computer Sci. & Engg, Jawaharlal Darda Institute of Engg. & Technology, Yavatmal, India.

Type of Review: Originality Check & Peer Review under the responsibility of the Scientific Committee of the Conference and The Institution of Engineers (India).
DOI: http://dx.doi.org/10.21013/jte.ICSESD201709

How to cite this paper:
Saturwar, J., Chaudhari, D. (2017). Performance Evaluation of watermarking Schemes to Decide Meaningful Number of Shares. *Proceedings of the International Conference on Science & Engineering for Sustainable Development (2017)*, 93-100. doi: http://dx.doi.org/10.21013/jte.ICSESD201709

ABSTRACT

With the growth in digital world, it is becoming more important to find a method to protect the security of digital media. An image watermarking model based on visual secret sharing (VSS) is proposed for protection of ownership. In the embedding phase, the watermark is first divided by VSS into two parts, a hiding watermark and a secret watermark. Then only the hiding watermark is embedded into the original image and the secret watermark is reserved for watermark extracting by the owner. In the extracting phase, the hiding watermark is extracted from the watermarked image first and then directly superimposed on the secret watermark to recover the watermark information. 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.

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

INTRODUCTION

A Digital watermarking is a covertly embedding technique of digital data with secret information that can be extracted by the recipient. The term "digital watermark" was first coined by Tirkel et al. The image in which the data to be hidden is embedded, is called the cover image or host. The watermarking process has to be resilient against tampering attacks, keeping the content of a watermark readable in order to be recognizable when extracted by the recipient. Features like robustness and fidelity are the essential features of a watermarking system; however, the size of the embedded information has to be considered as well since data becomes less robust as its size increases. Therefore, a trade-off between these features must be considered while developing a watermarking scheme. Generally, a complete digital watermarking system has three stages: watermark generation, watermark embedding, and watermark extraction for detection and authentication.

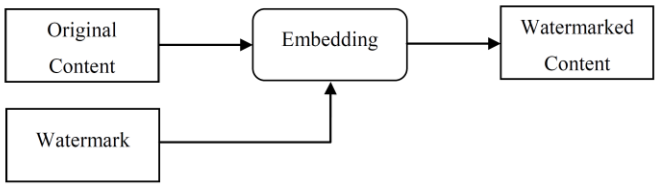

Figure 1. Water Marking embedding scheme

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 watermark 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.

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 watermark 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 watermark 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 have 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 that 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 binaryimages, 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 owner holds the other. 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.

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. Mathivadhani et al.
- A Self-Adaptive Blind Detection Color Watermarking Algorithm Based on Wavelet Contrast by Liu Dan.

B. Proposed Method

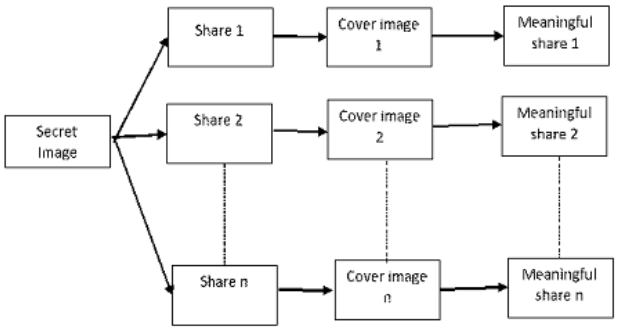

Figure 2: visual cryptography and watermarking model

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 θ 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 × 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 × 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 × N. Concatenation of these images will result in an N × 2N image.

The size of resulting shares would be 2N × 4N if Shamir's visual secret-sharing approach is used. However, the proposed method generates shares of size 2N × 2N with the same

hidingcapacity. 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

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 image 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.

		B	B	L
Lin-Tsai-		3	3	3
Yangetal.sc heme(PSN		4 1	4 1	4 1
Wangetal.sc heme(PSN		4 3	4 3	4 3

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 implemented for finding optimal number of shares. Most of the method was based on pixel expansion, which caused wastage of storage area. Some others have security problems. In the proposed VC schemes,security is provided to the secret shares and adversaries cannot alter its bit sequences to create fake shares. The vulnerability to 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 using watermark extraction technique.

REFERENCES

[1] *Adel Hammad Abusitta "A Visual Cryptography Based Digital Image Copyright Protection " Journal of Information Security 2012, (page no. 96-104) doi:10.4236/jis.2012.32012 Published April 2012 (http://www.SciRP.org/journal/jis)*

[2] *Jagdeep Verma, Dr.Vineeta Khemchandani "A Visual Cryptographic Technique to Secure Image Shares" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125*

[3] *B Surekhl,Dr GN Swamy, Dr K Rama Linga Reddy "A Novel Copyright Protection Scheme based on Visual Secret Sharing" ICCCNT'12 26th_28th July 2012, Coimbatore, India, IEEE-20180.*

[4] *Hui-Wen Liao "A Multiple Watermarking Scheme for Color Images" 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing 132-137.*

[5] *Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011 ISSN (Online): 1694- 0814 www.IJCSI.org*

[6] *B.Surekha, G.N.Swamy "Digital Image Ownership Verification Based On Spatial Correlation Of Colors" Int. Journal of Information assurance and Security,Vol 4,No 6,pp 470-473,2009*

[7] *Pradosh Bandyopadhyay, Soumik Das ,Prof Alai Chaudhuri, Dr. Monalisa Banerjee "A New Invisible Color Image Watermarking Framework through Alpha Channel" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012*

[8] *Saurabh Maheshwari, Reena Gunjan, Vijay Laxmi, Manoj S. Gaur "Robust Multi-Modal Watermarking Using Visually Encrypted Watermark" IWSSIP 2012, (page 72-75) 11-13 April 2012, Vienna, Austria ISBN 978-3-200-02328-4.*

[9] *Li Lianhuan ,Yao Yuxian Yang Xinfeng "Research on Adaptive Restoration Image Fragile Watermark Algorithm" 2011 International Conference on Computer Science and Network Technology December 24-26, 2011 IEEE (page no.1750-1753).*

[10]*Olcay Duman and olcay Akay "A New Method of wavelet Domain WaterMark Embedding and Extrection using Fractional Fourier Transform" (page no 187-191)*

[11]*HAN Yan-yan Xi'an China "A Watermarking-based Visual Cryptography Scheme with Meaningful Shares" 2011 Seventh International Conference on Computational Intelligence and Security 2011 IEEE (page no 870-873) DOI 10.1109/CIS.2011.196*

[12]*Ching-Lin Wang, Ching-Te Wang, Meng-Lin Chiang "The Image Multiple Secret Sharing Schemes Without Pixel Expansion" Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, 2011 (page no.1838-1844)*

[13]*Young-Chang Hou and Pei-Hsiu Huang "Image Protection Based On Visual Cryptography And Statistical Property" 2011 IEEE Statistical Signal Processing Workshop (SSP) ©2011 IEEE (page no.481-484)*

[14]*Ching-Sheng Hsu and Shu-Fen Tu "Digital Watermarking Scheme with Visual Cryptography" Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol IIMECS 2008, 19-21 March, 2008, Hong Kong ISBN: 978-988-98671-8-8 IMECS 2008.*

[15]*Shu-Chien Huang, Chu-Fu Wang "The Image Watermarking Technique Using Visual Secret Sharing Strategy" Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications(page no.190-195)*

[16]*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)*

[17]*Hao Luo1, Jeng-Shyang Pan2, Zhe-Ming Lu3, Bin-Yih Liao2" Watermarking-Based Transparency Authentication in Visual Cryptography" Seventh International Conference on Intelligent Systems Design and Applications, 0-7695-2976-3/07 © 2007 IEEE, pp 609-614*

[18]*Shu-Chien Huang, Chu-Fu Wang "The Image Watermarking Technique Using Visual Secret Sharing Strategy", Eighth International Conference on Intelligent Systems Design and Applications, 978-0-7695-3382-7/08 © 2008 IEEE pp.190-195*

[19]*Ankita Sengar , Preeti Verma "Digital Watermark performance with Visual Secret Sharing on either of RGB plane of colour image", 978-1-4673-1989-8/12 ©2012 IEEE*

[20]*Himanshu Sharma , Neeraj Kumar, Govind Kumar Jha "Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA)", International Conference on Computer & Communication Technology (ICCCT)-2011, 978-1-4577-1386-611©2011 IEEE pp 462-467*

[21]*F. Liu C.-K. Wu "Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners", Published in IET Information Security June 2010, IET Inf. Secur., 2011, Vol. 5, Iss. 2, pp. 121–128*

[22]*Mrs.D.Mathivadhani, Dr.C.Meena "Digital Watermarking and Information Hiding Using Wavelets, SLSB and Visual Cryptography Method", 978-1-4244-5967-4/10 ©2010 IEEE*

[23]*Aditya Vashistha, Rajarathnam Nallusamy, and Sanjoy Paul "NoMark: A Novel Method for Copyright Protection of Digital VideosWithout Embedding Data", 2010 IEEE International Symposium on Multimedia, 978-0-7695-4217-1/10 © 2010 IEEE pp.167-174*

[24]*S.Punitha, S.Thompson, N.Siva Rama Lingam "Binary Watermarking Technique based on Visual Cryptography", 978-1-4244-7770-8/10 ©2010 IEEE pp.232-235*

[25]*Chunhua Dong"A DWT-DCT Based Robust Multiple Watermarks for Medical Image", 978-1-4577-0911-1/12 ©2012 IEEE*

[26]*Arti , Harsh K Verma "Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based (k,n)-VCS",International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012*

[27]*Mustafa Ultas"Meaningful Shares Generation for Increased Number of Secrets in Visual Secret-sharing Scheme"Hindawi Punlishing Cooperation,volume 10,Article ID 593236.*