IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue- 7 E-ISSN: 2347-2693

Enhancing Visual Cryptography Using Digital Watermarking

Shobha Elizabeth Rajan[1*] *and* Sreedevi P[2]
[1*,2] *Dept. of Computer Science & Engg., MG University, India*

www.ijcseonline.org

Received: Jun/23/2015 Revised: July/06/2015 Accepted: July/24/2015 Published: July/30/ 2015

Abstract — The Visual Cryptography is an efficient cryptographic scheme which uses the human visual system (HVS) characteristics to decrypt images. But the factor that degrades its efficiency is that it is prone to attacks since OR or XOR operations are used for its decryption (HVS). In order to enhance the security factor of visual cryptographic scheme, watermarking of the encrypted images is proposed. Here we consider the Color Extended VC scheme and Intermediate Significant Bit (ISB) based watermarking technique. The shares produced through VC are watermarked on a host image and is made capable of securely transmitting through even attack prone communication channel.

Keywords— Visual Cryptography, Watermarking, ISB

I. INTRODUCTION

Visual Cryptography [1] is an emerging cryptographic technology. It provides information security through simple and less complex computations unlike other cryptography techniques. Visual Cryptography allows to encrypt visual information in a way that decryption can be performed using HVS [26]. There are many VC schemes introduced since 1997. Extended visual cryptography [2] is one of the enhanced VC scheme. It mainly involves two processes: encryption as well as decryption. Encryption is the processes of converting secret information into an unreadable form (using encryption algorithm). So that no one except those who have the special knowledge, usually referred to as a key can read the actual data. Without the correct key, the encrypted source content can't be detected by any unauthorized persons even though they steal the data. Decryption involves the reverse process of encryption in which the encrypted data is converted into its original form using decryption algorithm. Consider a situation where there is no need for decryption algorithm. Then we can reduce the complexity of mathematical calculations. There the concept visual cryptography arises. This type of visual cryptography technique perform reconstruction of the original data using simple OR operation. Fig: 1 shows a conventional Visual Cryptographic scheme.

Here each pixel of the original image is divided into four pixels. Among these four pixels two are white and two of them are black.

Shobha Elizabeth Rajan, shobharajan90@gmail.com
Department of CSE, MG university, India.
Sreedevi P, sree.dev@gmail.com
Department of CSE, MG university, India

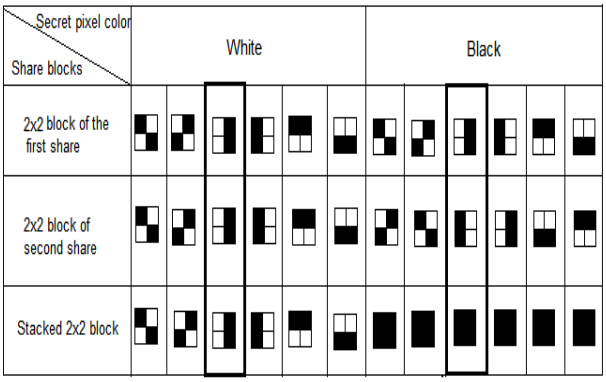


Fig 1: VC Scheme

Here each pixel of the image is separately scanned during encryption process. If the pixel is a white or a black select anyone of the six pixels shares shown in Fig 1,[1] for that corresponding pixel. Then put the selected pixel to one of the share and put the complement pixel share in the other share. Similarly perform the same operation for all other pixels to create the final shares. Each share alone gives no information about the pixel (whether it is black or white). The secret can be revealed only when both the shares are overlapped or superimposed.

For providing more security to this scheme an extended invisible digital watermarking technique [20] was employed. Using this technique, the divided shares obtained through secret sharing visual cryptography are embedded using ISB replacement. Here color change of the images cannot be sensed by human eye. This is a type of invisible digital watermarking as human eye cannot identify the change in the image. In the decryption process k number of images are taken and ISB are retrieved from each of them followed by OR operation to generate the original image. ISB based watermarking technique is used since it improves the robustness and quality of watermarked images.

II. RELATED WORKS

A. Extended visual cryptographic scheme

[2], [3] Describes the extended VC. Original images are provided as input and produces 'n' encrypted shares with the approximation of original images that satisfy the following three conditions:

- Any k out of n shares can recover the secret image.
- Any less than k shares cannot obtain any information of the secret image.
- All the shares are meaningful images; encrypted shares and the recovered secret image are colored.

Color Visual cryptography encryption method leads to meaningful shares. The method is simple and efficient. It relies on two fundamental principles for the generation of shares, namely, error diffusion and VIP synchronization [5]. VIP synchronization retains the position of the pixel carrying visual information. Error diffusion is an efficient algorithm for image halftone generation. Error diffusion generates shares pleasant to human eyes. The quantization error at each pixel is filtered and fed to future inputs. The error filter is designed in a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision.

B. Digital watermarking technique

In a digital image watermarking system [9] information carrying watermark is embedded in images. Ideally, it should be no perceptible difference between the watermarked and original image, and the watermark should be difficult to remove or alter without the degradation of the host image. A watermark usually is a binary sequence representing a serial number or credit card number, a logo, a picture or a signature. It is used to prove the copyright or ownership. Digital watermarking has become a significant topic of computer science due to the increasing popularity of the internet and the essential need of data security. In general, watermarking scheme [19], [23] consists of watermark embedding and watermark extraction. Embedding watermarking into the image is performed usually by modifying the image. It is often necessary to utilize Human Visual System (HVS) models for adaptively embedding the watermark. This can reduce the impacts of the modifications on image quality. Here the watermarking is performed using the bit plane replacement of ISB other than LSB [25] replacement techniques. A bit-plane of digital images is a set of bits having the same position in the respective binary numbers. In grey scale image representation, there are 8 bit-planes: the first bit-plane contains the set of the most significant bits MSB and the 8th bit-plane contains the least significant bits LSB. The set in between i.e. from 2nd to 7th bit-planes are intermediate significant bits ISB [4], as shown in Fig: 2 [4].

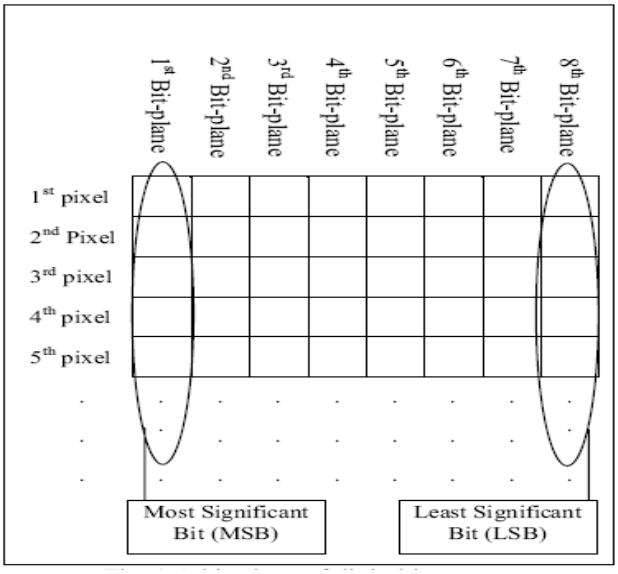


Fig. 2 A bit-plane of digital images

The value of each bit of the 8 bit-plane can be presented by 2n-1, where n is order of the plane starting from 1 to 8. i.e.: (20 + 21 + 22 + 23 + 24 + 25 + 26 + 27) = (1 + 2 + 4 + 8 + 16 + 32 + 64 + 128) = 255. The maximum value that can fit in 8 bits is 255 and the minimum value is 0. Any modification to the 8th bit-plane will change the pixel value by • ±1, the 7th bit-plane by • ±2, the 6th bit-plane by • ±4, the 5th bit-plane by • ±8, the 4th bit-plane by • ±16, the 3rd bit-plane by ±32, the 2nd bit-plane by • ±64, and the 1st bit-plane by • ±128. As a result, if the changed value is small (such as in 8th bit-plane), the image quality is kept high. While a big changed value (such as 1st bit-plane) causes the image quality to be highly degraded.

III. PROPOSED SYSTEM

The proposed method intended to enhance the VC scheme by incorporating the watermarking technique [12]. The process can be explained as follows: There are mainly two images to be considered:

- A secret information image (which is used for watermarking)
- A host image

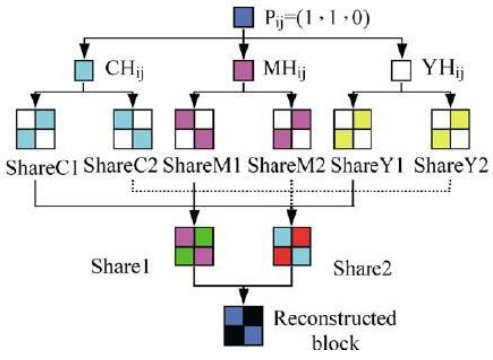
Initially consider the secret message information. The shares of the image is created using the VC scheme; in particular, Color Extended VC [5]. The shares obtained are considered for watermarking. This digital image is embedded into the host image. Watermarking consist of two

schemes; embedding and extraction. Since HVS model is employed for embedding the watermark, the method improves the need for modifying the visual quality of the image. Here one bit- plane is used to embed the watermark image into the selected bit-plane of the host. The bit-plane [6] of digital image is a set of bits having same position in the binary. Grey scale has eight bit-planes. For this the range [10] of the bit-plane is selected such that during embedding there is no change to pixels. If same range is not possible then the nearest range is selected. The best watermark is obtained at middle ranges. The methods for both VC and watermarking are explained below.

The method of VC needs the following steps:

1. Consider the color image.
2. Separate the images into three different color channels (RBG, CMY etc...).
3. Apply error diffusion for half toning.
4. Apply binary (2, 2) VC scheme.
5. Produce the shares.
6. Regenerate the original image

This method needs only two sharing image and does not sacrifice too much contrast for color visual cryptography. It transforms a color secret image into three halftone images [8] C, M, and Y and exploits the technique of gray-level visual cryptography to generate six temporary sharing images C1, C2, M1, M2, Y1, and Y2. Each of these sharing images will have two white pixels and two color pixels in every 2×2 block; i.e. all the color quantities are 24. The method then combines C1, M1, and Y1 to form a colored halftone Share 1 and C2, M2, Y2 to form Share2. So, for each block in Share 1 and Share 2, the color intensity is (12; 12; 12). After stacking Shares 1 and 2, the range of color intensity is between (12; 12; 12) to (1; 1; 1). Fig. 2 shows how to decompose a blue pixel (1; 1; 0) into two sharing blocks and how to reconstruct the blue-liked block.



In the encryption, the shares are generated from the color image. The color image is decomposed into R, G, and B channels. From these channels the shares are created.

Color Halftone: The color image "I" is decomposed into IR, IG and IB channels. Then apply halftone [11] for each channel to get halftone images. The color error diffusion is used for dithering technique. It reduces the color sets that render the halftone image and chooses the color from sets by which the desires color may be rendered and whose brightness variation is minimal. The error diffusion technique [5] is a dispersed dot dither method. In this method for each point in the image we find the closest color available and calculate the difference between the value in the image and the color. The two basic ways to scan the image are with a normal left-to-right and top-to-bottom raster, or with an alternative left-to-right and right-to-left raster. This algorithm scans through all pixels in the original image normally starting from the pixel left and then goes through all pixels from left to right and up and down. The value of each pixel in "I" is compared with a threshold. Normally, the value of threshold is 0.5 in the non-modified error diffusion. Depending on whether the pixel value is bigger or smaller than the threshold a 1 (black dot) or a 0 (white dot) is set at the corresponding position. The error is then diffused to a number of non-processed pixels. The diffusion of error is decided by an error filter. This method produces separate shares for RBG or CMY etc. Once the shares are obtained, watermark the shares on a host image. The steps could be simply explained as follows:

Step 1: Select the bit-plane one by one, from 0 to 8.
Step 2: Find the length of the range of the selected bit-plane by L = 2n-1 (n for 1st bit-plane is 8 while for 8th bit plane is 1)
Step 3: Create table ranges of the selected bit-plane (Number of ranges is 256 / L).
Step 4: For each range, two pixels are to be found: the maximum value of the range and the minimum value of the range, so that L = maximum value – minimum Value +1.

Step 5: Each range is divided into two equal groups; the length of each group is (L/2).
Step 5.1: In case the original bit is equal to the embedded bit, the distance d, between the original pixel and the nearest edge of the range, is to be found and the following steps are done:
Step 5.1.1: If the original pixel is in the left-hand group d = Original Pixel P – minimum pixel value of the range.
Step 5.1.2: If ($X \leq d$), the watermarked pixel P` = P. Otherwise, the watermarked pixel P` =minimum pixel value of the range + X.
Step 5.1.3: If the original pixel is in the right-hand group, d = maximum pixel value of the range original pixel P.
Step 5.1.4: If ($X \leq d$), the watermarked pixel

P=P. Otherwise, the watermarked pixel P` =maximum pixel value of the range – X.

Step 5.2: In case the original bit is different from the embedded bit, the following steps are to be done: If the original pixel is in the left-hand group, or in last range, the watermarked pixel, P` = maximum pixel value of the previous range –X.

Step 5.3: If the original pixel is in the right-hand group, or in the first range, the watermarked pixel P`= minimum pixel value of the next range + X.

Step 6: Calculate the PSNR and NCC for each embedding.

Step 7: If PSNR ≥ 30 db find the highest NCC and save the status which is considered the best status for embedding.

Watermark embedding in all bit-planes will be done with all possible bias values (X) (for every embedding the robustness and the quality of watermarked image will be measured). To improve the security of the system, the watermark object is encrypted using the shared key using the Data Encryption Standard (DES) algorithm.

Once the shares are extracted from the watermarked host image, the shares are decrypted to the original. In the decryption process the color image channels are reconstructed by stacking the shares of channels. These color image channels are combined to get the secret color image.

1) ***Stacking of Shares:*** The stacking (OR) operation is performed to recover the image of each channel.
2) ***Recovering the Image:*** The secret color image is recovered by performing the stacking (OR) operation between the shares S0, S1 i.e.

[S0, S1] Stacking → Recovered secret image.

IV. CONCLUSION

The paper aims to propose a method to enhance the quality of shares in VC scheme by watermarking the shares on to a host image. The VC is prone to hacking since decryption is done using Human Visual System. The proposed watermarking technique replaces the watermark image pixels that can protect the watermark data against attacks and at the same time keeping the new pixels very close to original pixels in order to keep the quality of the watermarked image. Compared to other VC schemes the proposed scheme provides more visual clarity on retrieved image.

REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, **1995**, (950):Page no(1-12).

[2] Dr.D.Vasumathi, M.Surya Prakash Rao, M.Upendra Kumar, Dr.Y.Ramadevi, Dr.R.Rajeswara Rao, "Novel Approach for Color Extended Visual Cryptography ," International Journal of Computer Trends and Technology- Volume-3, Issue4- **2012**.

[3] Kai-Hui Lee and Pei-Ling Chiu."An Extended Visual cryptography Algorithm for General Access Structures" IEEE Transactions on information Forensics and security,Volume- 7, No. 1,February **2012**.

[4] Akram M. Zeki and Azizah A. Manaf, "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit)", World Academy of Science, Engineering and TechnologyVol:3 **2009**-02-23.

[5] Color Extended Visual Cryptography using Error diffusion, InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee, IEEE Transactions on image processing, VOL. 20, NO. 1, JANUARY **2011**.

[6] M.Mohammed Sathik,"Feature Extracton on ColorED x-Ray Images by Bit- plane Slicing Technology Vol. 2(7), **2010**, 2820- 2824

[7] E. Verheuland H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes."Designs, Codes and Cryptography, 11(2), pp.179–196, **1997**.

[8] Y. C. Hou, "Visual cryptography for color images", Pattern Recognition, Vol. 36, pp.1619-1629, 2003.

[9] S.Punitha, S. Thompson and N.Siva Rama Ling "Binary Watermarking Technique based on Visual Cryptography " , 978-1-4244-7770-8/10/ **2010** IEEE .

[10] N.Ravia Shabnam Parveen, Dr. M.Mohamed Sathik, "Feature Extraction by Bit Plane Slicing Technique", in International Journal of Computing, Communication and Information System,Volume 1

[11] E.Sangeetha Devi, "Enhanced Visual Secret Sharing Scheme via Halftoning Technique", 978-1-4244-7770-8/10/**2010** IEEE.

[12] HAN Yan-yan and Xi'an China, "A Watermarking-based Visual Cryptography Scheme with Meaningful Shares", 978-0-7695-4584-4/11 **2011** IEEE.

[13] Vidyasagar M. Potdar, Song Han, Elizabeth Chang," A Survey of Digital Image Watermarking Techniques", 3rd International Conference on Industrial Informatics (INDIN),**2005**.

[14] Mauro Barni, Franco Bartolini, and Alessandro Piva**,** " Improved Wavelet-Based Digital Watermarking Through Pixel-Wise Masking ", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 5, MAY 2001**.**

[15] Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi, "A New Robust Watermarking Embedding into Wavelet DC Components", ETRI Journal, Volume 24, No. 5, October **2002**.

[16] C . S Rawat and Sneha M; S. "Watermarking Of Images Using Hybrid Technique"; International Journal of Application or Innovation in Engineering & Management (IJAIEM) ISSN 2319 - 4847 Special Issue for International Technological Conference-**2014**.

[17] Preeti Parashar1 and Rajeev Kumar Singh," A Survey: Digital Image Watermarking Techniques ",International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (**2014**), pp. 111-124.

[18] Sura Ramzi Sheriff ,"Digital Image Watermarking Using Singular Value Decomposition", Third Scientific Conference Information Technology Volume 7,No 3,**2010**.

[19] Voyatzis, G and Pitas, I. "Protecting Digital-Image Copyrights: A Framework", IEEE Trans. On Computer Graphics and Application, Volume. 19, No. 1, pp. 18-24, **1999**.

[20] Tripta Deendayal et al, "Enhanced Visual Cryptography Using Color Error diffusion and Digital Watermarking", Int. J. ComputerTechnology & Applications,Vol-3(1),261-264.

[21] Jayamohan, M., and K. Revathy. "A Hybrid Fractal-Wavelet Digital Watermarking Technique with Localized Embedding Strength." Wireless Networks and Computational Intelligence. Springer Berlin Heidelberg, **2012**. 584-591.

[22] A. J. Gonzalez, G. R. Arce, J. Bacca Rodriguez, and lD. L. Lau, "Human visual alpha-stable models for digital halftoning," in 18th Annual Symposium on Electronic Imaging Science and Technology: Human Vision and Electronic Imaging XI, San Jose, CA, Jan **2006**.

[23] R.B. Wolfgang and E.J. Delp, "A Watermark for Digital Images," Proc. IEEE Int'l Conf. Image Processing, vol. 3, pp. 219-222, **1996**.

[24] Ibrahim Nasir, Ying Weng, Jianmin Jiang," A New Robust Watermarking Scheme for Color Image in Spatial Domain", School of Informatics, University of Bradford, U.K.

[25] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE **2001**.

[26] S. H. Kim and J. P. Allebach, "Impact of HVS models On Model -based half toning," IEEE Transactions on Image Processing, vol. 11, pp. 258–269, Mar **2002**.

AUTHORS PROFILE

Sreedevi P is currently pursuing M.tech in Computer Science and Engineering from MG University, Kerala. B.tech Degree has been received from Kerala University.She has around 3yrs of experience in teaching field. Current field of interest is image processing, mainly in visual cryptography

Shobha Elizabeth Rajan is pursuing M.tech in Computer Science and Engineering from MG University, Kerala.B.techdegree hasbeen received from MG University. Current field of interest is image processing, mainly in visual cryptography.