Halftone Visual Cryptography & Watermarking

R.Charanya, T. Vijayan

Abstract:
In this Paper, a method of Information hiding & Piracy protection in Image processing is discussed. Visual cryptography & Digital watermarking helps in enables Information hiding, copyright & piracy protection. Here, a technique involving halftone visual cryptography along with watermarking is proposed to achieve visual cryptography via half toning. Digital watermarking is then performed to this halftone image. This ensures that the merits of both visual cryptography and watermarking are achieved. For visual cryptography, binary images are used for content protection. Here the image is spilt into shares which are randomly transmitted and then by means of visual decoding of information shares which are transmitted. From this process meaningful information is obtained.
Watermarking is an information hiding technique. The image or watermark is embed in the already obtained halftone image. Half-toning is done using the dithering algorithm.

Index Terms: Data Hiding, Dithering Principles, Halftone Imaging, Image Processing, Privacy Protection, Visual Cryptography, Watermarking

1 INTRODUCTION

Due to rapid development of networks such as Internet, Intranet, Wireless Communication, global mobility networks, World Wide Web etc & multimedia techniques, digital data such as text, image, video & audio has now been widely used.

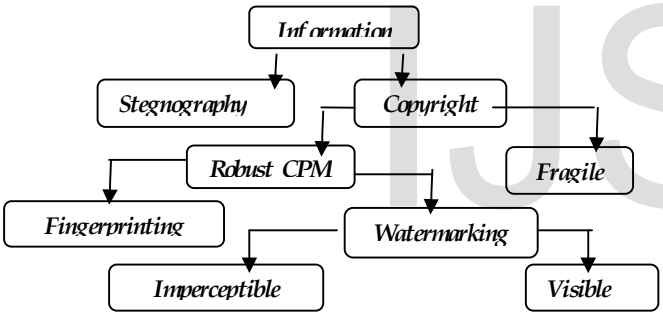


Fig 1.1 Classification of information hiding techniques

Many techniques have been developed to protect the property against the piracy; these techniques are called information hiding. To protect intellectual property in both digital and print media, one of the methods known as watermarking technique is used.

1.1 Visual Cryptography

Visual Cryptography is a technique of cryptography which enables the decryption of images without using computer. One of the most sought out techniques developed were that of Moni Naor & Adi Shamir which is most prevalently used. In this scheme of VC, a secret binary image (SI) is cryptographically encoded into shares of random binary patterns. They can be some random noise images or images with some rough foreground in [3].
Algorithms are available to hide a secret image between a grayscale image and a random noise image. These shares are then Xeroxed onto transparencies, respectively, and distributed amongst participants, one for each participant. Each participant will not know the share given to the other, this ensures secrecy. The required image can be revealed by superimposing of the n transparencies together.

1.2 Halftoning

Half toning is a reprographic technique that creates continuous tone imagery by the use of dots, varying either in size, in shape or in spacing. It is a process for changing multi-tone images into two-tone images, which look like the original multi - tone images when viewed from a distance. They are widely used in the printing of books, magazines, newspapers, and in computer printers. Continuous tone images are those which contain infinite ranges color in grey scale.

Digital half-toning uses a raster image or bitmap within which each monochrome picture element or pixel may be on or off, ink or no ink. Consequently, to emulate the photographic halftone cell, the digital halftone cell must contain groups of monochrome pixels within the same-sized cell area. The fixed location and size of these monochrome pixels compromises the high frequency/low frequency dichotomy of the photographic halftone method. Clustered multi-pixel dots cannot "grow" incrementally but in jumps of one whole pixel. In addition, the placement of that pixel is slightly off-center. To minimize this compromise, the digital halftone monochrome pixels must be quite small, numbering from 600 to 2,540, or more, pixels per inch. However, digital image processing has also enabled more sophisticated dithering algorithms to decide which pixels to turn black or white, some of which yield better results than digital half toning.

1.3 Watermarking

Watermarking is an image data hiding scheme. Here the hiding or embedding of invisible data in an image without affecting the actual image quality such that the hidden data can be extracted with some procedure is done. Digital watermarking aids owners in asserting their intellectual property rights on the works of art they create. These rights are particularly difficult to enforce with digital images, since it is easy to copy and distribute perfect copies of an original image. Fig1.2. shows the basic components of any watermarking technique.

- *R.Charanya is currently pursuing masters degree program in Electronics & Instrumentation Engineering in Bharath University, India, PH-+919176638538. E-mail: charanya_147@yahoo.in*
- *T. Vijayan is working currently as Asst. Prof. in Bharath University, India, PH-+919894857331. E-mail: vijayanthiruvengadam@gmail.com*

It consists of:

- *A Watermarking algorithm that inserts information,*
- *The watermark, into an image.*

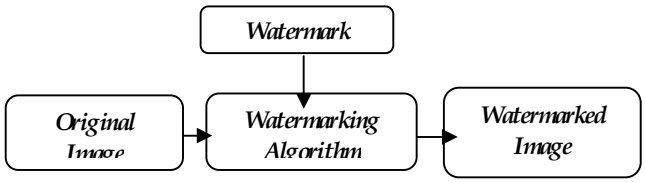


Fig 1.2. Block diagram of a watermarking algorithm

The watermark is inserted into the image in the spatial domain or spatial frequency domain. As part of the watermarking technique, a testing algorithm must be defined that tests an image to see if a particular watermark is contained in the image. It is also desirable for the testing procedure to determine if the image has been altered and to supply localization information as to where the image was altered. It is our feeling that to assert ownership that is consistent with current intellectual property right law, the watermarking technique must support the use of third-party cryptographic-based digital time stamping that is embedded in the image through the watermarking process.

2. HALFTONE VISUAL CRYPTOGRAPHY

In order to understand the principles of VC, we consider a two out- of-two visual scheme where each pixel P of the binary image is encoded into a pair of sub pixels in each of the two shares. Two cases are possible; the color chosen can be either white or black. Each of the 2 cases we have 2 types of combinations giving 2 types of output each totally 4 as shown in fig 2.1. Here, the selection is performed in a manner like randomly flipping a fair coin, such that each column has an equal probability of 1/2 to be chosen. Sub pixels are then obtained and the same is tabulated as Share 1 & Share 2. Each share is encoded as a pair of equal probabilities thus there is no use of viewing each share separately [1].

Pixel		Share 1	Share 2	Result
	P=1/2			
	P=1/2			
	P=1/2			
	P=1/2			

Fig 2.1: Visual cryptography

If we see fig 2.1, the 1st column shows the 2 types of image pixel possible, black or white. The next column gives us the probability of the pixel P= ½ which is the same for both. The next 2 columns give the combination of share 1 & share 2. Now consider the superposition of the two shares as shown in the last column of Fig. 2.1. If a pixel is white, the superposition of the two shares always outputs one black and one white sub pixel, no matter which column of sub pixel pairs is chosen during encoding. If is black, it yields two black sub pixels. There is a contrast loss in the reconstruction; however, the decoded pixel is readily visible.

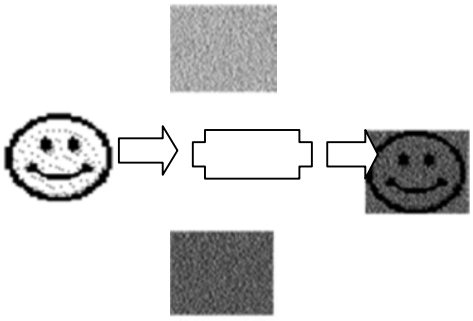


Image Split as 2 Shares ==Decoded image

Fig:2.2 VC Scheme

Fig2.2 shows a basic visual cryptography scheme where an image is split into 2 shares & then is decoded back & given. It is observed that, the width of the decoded image is more than that of the input image ie the pixels undergo stretching.

2.1 Dithering Principles

Halftoning is the process of changing a greater amplitude resolution to the one with lower resolution. Various methods are available for this purpose of which the dithering algorithm is illustrated in this paper. Dithering is commonly used to convert a gray scale image to a halftone, which is bi-tonal. The illusion of a gray scale image is created by the pattern of black and white dots. The ordered dithering method using a halftone dithering matrix is used here.

Dithering reduces the Z-resolution, or number of quantization levels, of the components in a continuous tone image. It simulates the visual appearance of the original image by substituting the original continuous tone data with fixed patterns of lower Z-resolution data.

The purpose of dithering is generally to match the number of quantization levels in an image with those of a display device. For eg, to display a gray scale image that has 256 levels on a workstation that displays only 8 levels, you would dither the image so it only has 8 levels. Dithering uses a neighborhood operation on each pixel to assign it one of the 8 values. It attempts to preserve the illusion of an image with 256 levels by creating a pattern, or screen, of dots (representing 8 intensity levels) to represent an intensity level.

2.2 Algorithm for 2 out of 2 schemes

Step1- Input the original pixel S_{ij}.
Step2- Pixel reversal is applied
Step3- Use random number generator (0.1 to 0.9) to reduce Si j´ randomly & take the difference of Si j´ with original pixel Sij.
Step4- Use random number generator to reduce reversed value of Si j´ randomly & apply pixel reversal i.e. Si j´´
Step5- Store in matrix as image called share1.

Step6- Take the difference of two random number generators with original pixel Si j & again reverse the pixels to get Si j´ ´ ´
Step7- Store Si j´ ´ ´ in matrix as image called share 2.
Step8- Repeat steps for all pixel from original image (i.e. matrix of original image)

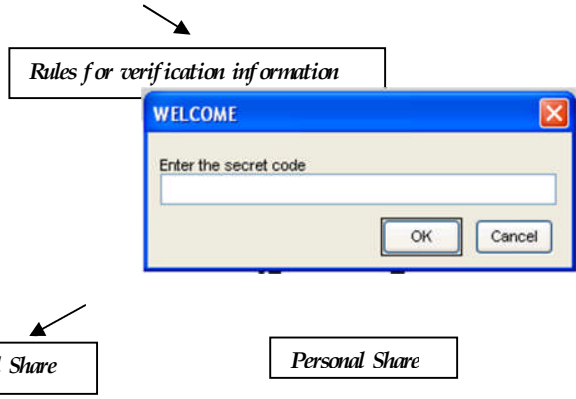
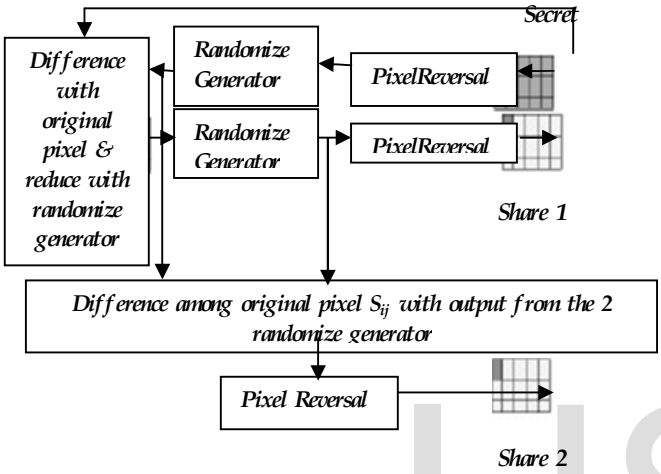


Fig 3.1 Water marking Algorithm using Visual Cryptography concept: Watermarking embedding process.



3. WATERMARKING & HALFTONING

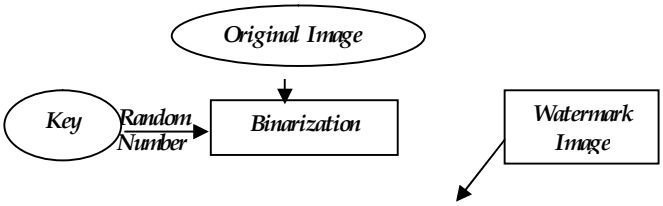
A digital watermark as already seen, is a kind of marker embedded in an audio or image signal, typically used to identify ownership of the copyright of such signal. An algorithm that combs both Half-toning & watermarking process in one can be used. Modified algorithms operate on halftone images and the modification includes both classification and extraction of watermarks [13]. Moreover, we use NXOR instead OR to improve accuracy of the extracted watermarks. To retrieve the watermark, original image is not required; however a secret of watermark (secret key) is needed. Another requirement is that the embedded watermarks must be invisible to human eyes and robust to common image processing attack operations. For this reason, a watermark is repeated all over the image to avoid attacks such as filtering and image cropping.

The watermarking process can be written by the following equation:

$$Hw = H + f(H,w)$$

Where, H is the host image, Hw is the watermarked image, w is the watermark image and 'f' the watermarking function.

There are two methods for the embedding of the watermark in the host image known as image dependent & image independent methods



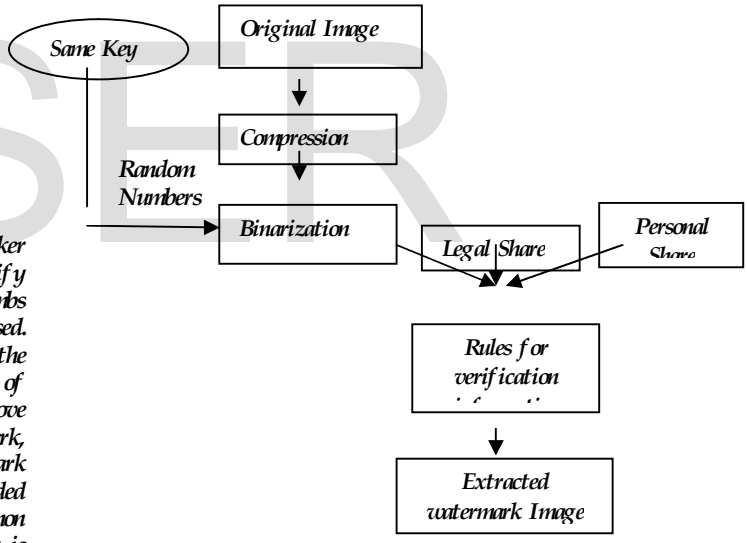


Fig 3.2 Watermarking extraction process

4. RESULTS

Here, a multitone image is taken and converted into a 2 tone image. The 2 tone image is then watermarked for various quality factors. Images that are used during these experiments, dimensions, sizes and the compression ratio are listed in the Table 1

TABLE 1
IMAGES & THEIR COMPRESSION RATIOS

Image	Image type	Dimensions	Size	Compression ratio
Baby(gray)	Jpeg	516x368	22.1KB	8.3710
Baby(Binary)	Jpeg	516x368	35.4 KB	5.2243

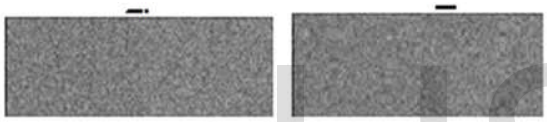
Share 1	Jpeg	778x277	934 KB	22527
Share 2	Jpeg	778x277	934KB	22527
Decoded	Jpeg	778x277	383 KB	54919

(a).Original Image (b) Halftone Image

The actual principal involved in visual cryptography will be shown stage by stage by using a secret code/key.

(c) Key/ secret code
Fig 4.1 Half tone Visual cryptography

If the entered code is valid then it show Fig4.2(a) to 4.1 (d), otherwise display Invalid code



(a) Share 1 (b) Share 2

(c) Decoded Image (OR operation)

(d) Decoded Image (XOR operation).

Fig. 4.2. Simulation results for image sharing using visual cryptography

RESULTS FOR WATERMARKING IN HALFTONE IMAGES

A basic Watermarking algorithm[8] was implemented to hide an image inside a picture. The results obtained are as shown below:

Fig. 4.3(a) Input Image (b) Watermarked Image with Noise. (c) Watermark which has been embed

Here the image output which is obtained can be further analyzed based on quality factor specification of the image. The output shown in fig 4.3 indicates as to how image quality varies depending on quality factor.

Menu display shown below, depending upon the quality factors the extracted watermark and watermarked Image can display in the following figures.

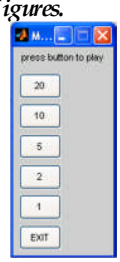


Fig. 4.4 a) Original Image (b)Watermarked Image c) Watermark Image of halftone image with quality factor=20

Fig. 4.5.(a) Original Image, (b) Watermarked Image (c) Watermark Image of Halftone Images with quality factor=05

Fig. 4.6.(a) Original Image (b) Watermarked Image (c) Watermark Image of Halftone Images with quality factor=01

5. CONCLUSION

In this paper, a general framework of halftone visual cryptography is discussed. The dithering principle is applied to create half tone VC, carrying significant visual information. This method can be used in applications that require high quality images

The expansion of Internet has made large amount of digital information available to the mass. Though the Internet technology has improved the every day's life, it also makes unauthorized copy and distribution of multimedia data much easier. In these circumstances, there is a strong need for copyright protection and a considerable interest in identifying methods for inserting a "digital signature" called "watermark" which can be used to identify the owner to discourage unauthorized document copying and distribution and possible, to earn royalties.

A simple and efficient watermarking algorithm using Image Sharing principle, which is used to provide copyright protection for any digital image, is proposed in this project. Using Visual Cryptography, the Image containing the author information (Secret Image) is divided into two shares using a key in such a way that, it is impossible to predict the second share from the first share. One share will be kept with the author and the other with a legal body. It has been proved that the proposed watermarking algorithm is tolerant to high level of JPEG compression. It can also be seen from the results obtained that the quality of image varies according to the quality factor specified by the user.

REFERENCES

[1] Zhi Zhou, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo "Halftone Visual Cryptography" IEEE TRANSACTIONS ON IMAGE PROCESSING,, AUGUST 2006

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoret. Comput. Sci., vol. 250,no. 1–2, pp. 134–161, 2001.

[3] M. Naor and A. Shamir, "Visual cryptography," Adv. Cryptol: EUROCRYPT,Lecture Notes Comput. Sci., vol. 950, pp. 1–12, 1995.

[4] "Visual cryptography II: Improving the contrast via the cover base," in Security in Communication Networks, Lecture Notes in Computer Science. Amalfi, Italy: , 1996, vol. 1189, pp. 197–202.

[5] C. Chang and H.Wu, "A copyright protection scheme of images based on visual cryptography," Image. Sci. J., vol. 49, no. 3, pp. 141–150, 2001.

[6] C.Wang, S. Tai, and C. Yu, "Repeating image watermarking technique by the visual cryptography," IEICE Trans. Fundam. Electron. Commun.Comput. Sci., vol. E83A, no. 8, pp. 1589–1598, Aug. 2000.

[7] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptol: J. Int. Assoc. Cryptol. Res., vol. 12, no. 4, pp. 261–289, 1999.

[8] Vikas Tyagi, "Data Hiding in Image using least significant bit with cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, vol 2 issue 4, april 2012.

[9] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math.,vol. 16, no. 2, pp. 224–261, 2003.

[10] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," Theoret. Comput. Sci., vol. 240, no. 2, pp. 471–485, Jun. 2000.

[11] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[12] R.A. Ulichney, Digital Halftoning, Cambridge, MA:MIT Press, 1987.[3]Ping Wah Wong, Nasir D. Memon, "Image processing for halftones", IEEE Signal Processing Magazine, July 2003, vol. 20, No. 4, pp. 59-70.

[13] Ming Sun Fu. Oscar C. Au*Joint visual cryptography and watermarking IEEE International Conference on Multimedia and Expo (ICME) pp 975-978, 2004,

[14] Rafael C.Gonazalez, Richard E.Woods, Steven L.Eddins "Digital Image Processing Using MATLAB" pearson Education.

[15] Anil K. Jain "Fundamentals of Digital Image Processing" Prentice Hall of India.