AN EFFECTIVE METHOD FOR IMPROVING THE VISUAL QUALITY OF GRAYSCALE IMAGES

LENNY ZENO.S, NIJA SHINING GOLD T.L, DR DEEPA A. J

M.E,ASSITANT PROFESSOR, [3]HEAD OF THE DEPARTMENT
COMPUTERSCIENCE AND ENGINEERING,
PONJESLY COLLEGE OF ENGINEERING, NAGERCOIL, INDIA.

Abstract

Visual cryptography is a technique to hide the data by using encryption and decryption method. Visual Cryptography is a cryptographic techinque which allows visual information(picture, text ,etc.) to be encrypted in such a way that the decryption can be performed by human visual system It is a kind of secret sharing scheme where the secret is in the form of an image. It is split into random shares and distributed to the participants. These random shares individually don't reveal any information of the secret image. This reduces the quality of the recovered image Pixel expansion increases the size of the shares and creates inconvenience for the participants while carrying the shares. secret image and the visible image are first converted to halftone image using Halftone error diffusion method. visual cryptography, the secret share images are transformed into meaningful shares.

Keywords: Error diffusion, Halftone visual cryptography (HVC), Halftoning, Visual cryptography (VC), Cryptography, Secret sharing.

INTRODUCTION:

Visual cryptography is a cryptography technique which allows visual information to be encrypted in such a way that the decrypted information appears as a visual image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. The shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye. Sharing a secret with an arbitrary number of people N such that at least 2 of them are required to decode the secret is one form of the visual secret sharing scheme presented by moni naor and adoar Shamir in 1994[1]. In this scheme we have a secret image which is encoded into N shares printed on transparencies [1]. Every pixel from the secret image is encoded into multiple subpixels in each share image using a matrix to determine the color of the pixels. Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications.

The secret shares as well as the recovered image will be m times larger than the secret image [3]. This reduces the quality of the recovered image Pixel expansion increases the size of the shares and creates inconvenience for the participants while carrying the shares. Many algorithm of visual cryptography were proposed to overcome this practical problems. There are certain method used to improve the visual quality of the image . while processing a digital image, the most convenient, the most convenient color model used is the grayscale model. There are several algorithms approximating this transformation, but none of them can be truly perfect, since those colors are simply out of the target device's capabilities. This is why identifying the colors in an image which are out of gamut in the target color space as soon as possible during processing is critical for the quality of the final product. Grayscale image is used carry an intensity information is one in which the value of each pixel is a single sample .grayscale image can be the result of measuring the intensity at each pixel according to the particular weighted combination of frequencies.

2. GAMMUT MAPPING.

The gamut mapping is used to improve the quality of the image. The modification process is said to gamut mapping. So in a local block, the dynamic range is halved , for each pixel is zero.The gamut of reflective colors in nature has a similar, though more rounded, shape. To ensure a good correspondence of overall color appearance between the original and reproduction by compensating for mismatch in the size ,shape and location .it is used to preserve the axis of the image and aim it to produce maximum of the contract of the same quality .it is used to increase the saturation is preferred. Depending upon the parameter ,setting different type of information can be used to estimate the illuminant. the goal is to transformation that minimize negative visual effect. to minimize or to maximize the color that depend upon apply. Various gamut mapping algorithm are used among that specifically SIG-LIN is used in this , to specify the quality of the image used.

3.QUANTIZATION

Quantization , involved in image processing is an low compression technique achieved by compressing a range of value to a single quantum values. When the number of discrete symbols given in a stream is reduced.

4.DIGITAL HALFTONING

It is similar to halftoning in which is an image is decomposed into grid of halftone cell. There are three types of the *digital* halftones cell . there are patterning dithering ,error diffusion error diffusion is a type of halftoning in which the quantization residual is distributed to various operation like dithering etc. in this the current pixel is used to compare with to half –gray value.

5.VC ENCRYPTION

Vc encryption is a techinque used to generate share s1,s2….sn. it is used to generate share x number of share. large number of pixel of an image cannot be visible. In an image visual pixel cannot be visible .

6.PROBABILISTIC SIZE INVARIANT VISUAL SECRET SHARING SCHEMES

In probabilistic mode, each pixel is reconstructed with a single pixel. So, the reconstructed image is size invariant without any pixel expansion. The secret can be reconstructed only with certain probability in the probabilistic model. The quality of the reconstructed pixel depends on how big the probabilities are of correctly reconstructing the secret. Ito et al [4] has proposed a size invariant (k,n) VSS, k is the threshold shares and n is the total shares. The structure of Ito et al's scheme is constructed by using two sets of n X m Boolean matrices C0 and C1. Two nXm matrices S0 and S1 are randomly choosen from C0 and C1 and to share a white pixel one of the coloumns of S0 and to share a black pixel one of the coloumns of S1 are chosen randomly . The column vector is described by a Boolean n-vector V = [vi], vi= 1 for a black pixel and 0 for a white pixel in the ith share. During the stacking up of shares, the color of the pixel is determined as "OR"ed value of the corresponding elements in V .p0 and p1 are the probabilities with which a black pixel in the reconstructed image is generated from a white and black pixels respectively, in the secret image. Thus, the reconstructed image can be recognized as a secret image by the contrast as the absolute difference in the probabilities β|p0-p1| .This is a secure scheme and the reconstructed image is well visible. The Boolean matrices used by Ito in (k,n) scheme is as follows with S0 as nxn matrix having one column with 1's and all other columns as 0's and S1 as a unit matrix.

Probabilistic Size invariant visual secret sharing schemes[4,5,6] for a binary image use only one subpixel to share the secret image i.e. each pixel is encrypted individually or independently in a probabilistic manner. Thus, the generated shares has the same size as the secret image, thus it is size invariant. Ito[4] in 1999 proposed a method of (k,n) probabilistic scheme by using the basis matrix used by Shamir in traditional visual Cryptography. The probabilistic method proposed by Yang[5] uses the frequency of white pixels to show the contrast of the recovered image. Random grid[9] scheme is another method, which encodes a secret image into two noise-like images, where each image is referred as a Random Grid. The size of a RG is the same as that of the secret image ie. without pixel expansion. However, a reconstructed secret has lower visual quality in RG-based VC. To improve the visual quality of the recovered image and reduce the number of operations, multipixel[10,11] encryption strategy was proposed. Multipixel encryption methods grouped the pixels into blocks and encrypted the blocks at a time. This also improves the visual quality of the recovered image.

This paper provides an analysis of various size invariant visual cryptography schemes like probabilistic scheme[4-6], random scheme[7] and multipixel[8-11] encryption. The paper is organized as follow: Section 2 defines the traditional visual cryptography. The next 3 sections provides the overview of probabilistic ,random grids and multipixel size invariant schemes. The performance of (n,n) size invariant visual cryptography schemes, where n=2 i.e,(2,2) are analyzed and results are tabulated in section 6, followed by conclusion.

7. RANDOM GRIDS SCHEME

A simple technique for encryption of 2-D patterns was proposed by Kafri and Karen [7]. This is a (2,2) scheme.This method can encrypt a binary image into two shadows images, called random cipher grids. The number of pixels in the encrypted shares are same as the original secret. In Visual Cryptography, each image pixel is represented as either transparent (white) or opaque (black). The two type of pixels are likely to occur. Light is transmitted through the transparent pixel, while the opaque pixel stops it. Depending on the characteristics of the shadows in the random grids, Kafri et al. proposed three visual secret sharing algorithms using random grids that differ from each other in their contrast quality.

8. . MULTIPIXEL ENCRYPTION SCHEME

The multi pixel encryption scheme is a size invariant scheme. Instead of encrypting a single pixel at a time, few pixels are blocked together and encrypted at a time and divided into shares.

Definition 2 A (k, n)-Prob. VSS scheme can be shown as two sets, white set C_0 and black set C_1, consisting of n_λ and n_γ $n \times 1$ matrices, respectively. When sharing a white (resp., black) pixel, the dealer first randomly chooses one $n\times1$ column matrix in C_0

(resp., C_1), and then randomly selects one row of this column matrix to a relative shadow. The chosen matrix defines the color level of pixel in every one of the *n* shadows. A Prob. VSS Scheme is considered valid if the following conditions are met.

For these n_λ (resp., n_γ) matrices in the set C_0 (resp., C_1) the "OR"-ed value of any *k*-tuple column vector *V* is *L*(*V*). There values of all matrices form a set λ (reps. γ). **Definition 3** : A (k, n, t)-Multi-pixel encryption size invariant visual cryptography scheme encrypts a block of t adjacent pixels at a time, where the chosen of the t pixels does not relate to the content of the secret image. For the encryption of any two blocks B and B_1 in the secret image, a (k, n, t)-ME-SIVCS-2 generates n shares s_1,……,s_n satisfying.

1. (Contrast) Denote v and v' as the vectors that consist of the secret pixels at B and B' respectively, and denote v_p and v'_p as their corresponding vectors that are no the shares S_p for P= 1, ………, n. Without loss of generality, suppose w(v) > w(v'), then for any k out of n shares {s_{q1}, …….., s_{qk}} (□ {s_1, ……, s_n}), let $V_Q = v_{q1}$ OR, ……, OR v_{qk} and $V'_Q = v_{q1}$ OR, ……, OR v'_{qk} then stacking result satisfies > where for example is the average values of w(v_Q) for all the possible values of v_Q.
2. **Algorithm 1**: The first shadow RG_1 is generated randomly by the bits 0 or 1 . The size of this share is same as the secret image. Then, if the secret binary pixel SI(i, j) is equal to 0, the binary pixel of the second shadow RG_2(i, j) at the same position will be the same as in RG_1(i, j); otherwise, the binary pixel in RG_2 (i, j) will be the complement of RG_1 (i, j).
3. **Algorithm 2**: The first shadow RG_1 is generated randomly by the bits 0 or 1. The size of this share is same as the secret image. Then, if the secret binary pixel SI(i, j) is equal to 0, the binary pixel of the second shadow RG_2 (i, j) at the same position will be the same as in RG_1(i, j); otherwise, the binary pixel in RG_2 (i, j) will be generated randomly by the function

Algorithm 3: The first shadow RG_1 is generated randomly by the bits 0 or 1. The size of this share is same as the secret image. Then, if the secret binary pixel SI(i, j) is equal to 0, the binary pixel in RG_2 (i, j) will be generated randomly by the function otherwise, the binary pixel in RG_2 (i, j) will be the complement of RG_1 (i, j).

AUTHORS AND AFFILATION

LENNY ZENO.S, NIJA SHINING GOLD T.L, DR.A.J.DEEPA

[1] M.E,[2]ASSITANT PROFESSOR, [3]HEAD OF THE DEPARTMENT
[1]COMPUTERSCIENCE AND ENGINEERING,
[1]PONJESLY COLLEGE OF ENGINEERING,[1] NAGERCOIL, [1]INDIA

CONCLUSION

The random grid and probabilistic method are used to determine to improve the quality of the given image.to improve ethe size-invariance, the size invariance algorithm is used within the random grid method . the random gird method are used to determine the size of the image improvement .from thee experiments ,they are determined.

REFERENCES

[1] A. Shamir(1979), How to share a secret, *Comm. ACM,* 22(11):612–613

[2] G. R. Blakley(1070), Safeguarding cryptographic keys, *AFIPS 1979 Nat. Computer Conf.*,48:313–317

[3] M. Naor and A. Shamir(1995), Visual cryptography,*In Advances in Cryptology-EUROCRYPT'94*, page 1. *Springer*

[4] Ito, R., Kuwakado, H., Tanaka H(1999), Image size invariant visual cryptography, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 82(10),* 2172–2177

[5] Yang, C.-N. (2004), New visual secret sharing schemes using probabilistic method, *Pattern Recognition Letters 25(4)*, 481–494

[6] Cimato, S., Prisco, R.D., Santis, A.D(2006), Probabilistic visual cryptography schemes, *Comput. J.* 49(1), 97–107

[7]0. Kafri and E.Keren(1987), Encryption of pictures and shapes by random grids, *Optics Letters*, vol.12,no.6,pp.377-379

[8] Feng Liu, Teng guo, ChuanKun, Lina Qian(2012), Improving the visual quality of size invariant visual cryptographic scheme, *Journal of Visual Communication and Image Representation*, vol 23, Issue 2,pp331-342

[9] Y.W Chow, W Susilo, D.S Wong(2012), Enhancing the perceived visual quality of size invariant visual cryptography scheme, *Information and Communications Security, Springer LNCS,* vol 7618,pp10-21 , 2012 .

[10] Nazanin Askari, Cecilia Moloney, H.M. Heys(2012), A Novel Visual Secret Sharing Scheme without Image Size Expansion, *25th IEEE Canadian Conference on Electrical and Computer Engineering*

[11]C.L. Wang and C.T. Wang and M.L. Chiang(2012), "The image multiple sharing schemes without pixel expansion", *International Conference on Machine Learning and Cybernetics*, Guilin,

[12]C.L.Chou(2002),A Water marking Technique based on non-expansible Visual Cryptography,*Thesis,* Department of Information Management, National Central University.