Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Shraddha Gupta, IJPRET, 2014; Volume 2 (9): 1098-1103 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

VISUAL CRYPTOGRAPHY FOR IMAGES

MS. SHRADDHA SUBHASH GUPTA[1], DR. H. R. DESHMUKH[2], PROF. S. A. KARADE [3]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Prof and HOD, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
3. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Security has become an inseparable issue even in the field of space technology. Visual Cryptography is the study of mathematical techniques related aspects of Information Security which allows Visual information to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This technique represents the secret image by several different shares of binary images Some predefined set of participants can decode a secret message without any knowledge of cryptography and without performing any cryptographic computation. Their visual system will decode the message. It is hard to perceive any clues about a secret image from individual shares. The secret message is revealed when parts or all of these shares are aligned and stacked together In this paper we provide an overview of the Visual Cryptography (VC) technique used in the secure transfer of the thousands of images .The related work is based on the recovering of secret image by visual cryptography algorithms.

Keywords: Visual Cryptography (VC), Halftone, Dithering

PAPER-QR CODE

Corresponding Author: MS. SHRADDHA SUBHASH GUPTA

Access Online On:

www.ijpret.com

How to Cite This Article:

Shraddha Gupta, IJPRET, 2014; Volume 2 (9): 1098-1103

INTRODUCTION

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.

When the random image contains truely random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other[3].

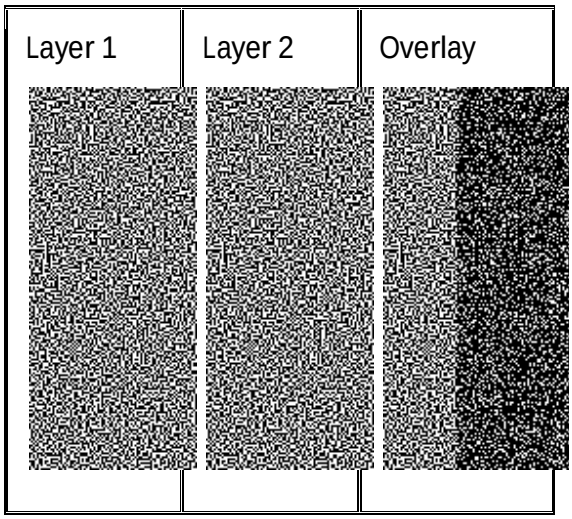

Fig 1. Overlaying of Layers.

II.MATERIAL AND METHOD

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

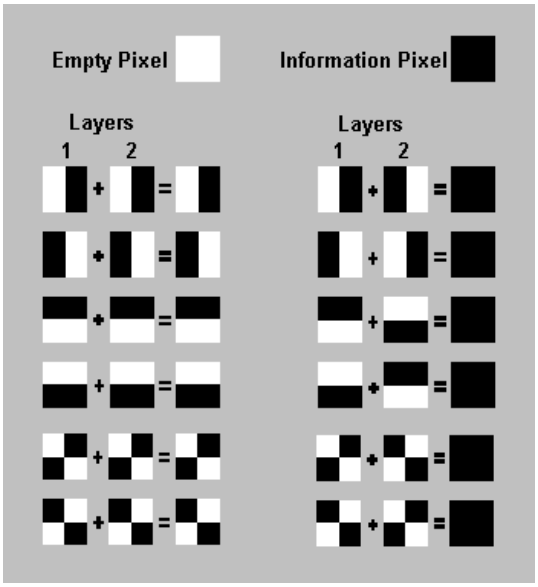

Fig 2. Pixels of images.

In the table on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel. We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory[1].

III. TYPES OF VISUAL CRYPTOGRAPHY.

1. Blue noise dithering: This technique is used to improve the quality of image during reconstruction of the image .

2. Void cluster algorithm: This technique is used to find the secret pixel in the halftone cell .

3.Halftone: It is a production of graphic through mechanical or electrical such as photography or xerography techniques that simulates images where each color can be reproduced as single tone in monochromatic print. In proposed method, the secret image can be decoded without showing any interaction with share image[5].

IV. VISUAL CRYPTOGRAPHY (2,N) SHARING CASE

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 Adi Shamir in 1994. In this scheme we have a secret image which is encoded into N shares printed on transparencies. 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.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. In the (2,N) case a white pixel in the secret image is encoded using a matrix from the following set:

$$\mathbf{C_0} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \dots & & & \\ 1 & 0 & \dots & 0 \end{bmatrix}.$$

{all permutations of the columns of} :

While a black pixel in the secret image is encoded using a matrix from the following set:

$$\mathbf{C_1} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & & & \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

{all permutations of the columns of} :

For instance in the (2,2) sharing case (the secret is split into 2 shares and both shares are required to decode the secret) we use complimentary matrices to share a black pixel and identical matrices to share a white pixel. Stacking the shares we have all the subpixels

associated with the black pixel now black while 50% of the subpixels associated with the white pixel remain white[4].

V. COMPLEXITY WITHIN VISUAL CRYPYOGRAPHY.

Many of the proposed schemes in VC result in share sizes that grow very large depending on the image size and type. Typically as the contrast improves the share size also increases quite dramatically. This increases image processing times which increases the overall complexity of the scheme. By increasing this complexity it reduces the overall potential for a practical application of VC. Share sizes become completely unmanageable, specifically when high resolutions are used to share information.

Sharing large amounts of information also presents another complexity ,hiding single works or phrases within the shares has proven to be effective. However if a larger amount of data is required to be shared such as a paragraph of text the share sizes again become unwieldy and difficult to manage.

Tackling this complexity has been a real challenge within VC. There are a number of schemes which present near optimal solutions for share sizes [20,131,132] ,but many schemes produces share sizes that are problematic in terms of practical use[6].

VI. CONCLUSION

Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc.. The decoded secret image quality is improved. Undoubtedly, Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. 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. The overlapping of these shares reveals the original secret. The decoded secret image quality is improved.

VII. REFERENCES.

1. M. Naor, A. Shamir, in: A. De Santis (Ed.), VisualCryptography, Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer,Berlin, 1995.

2. M. Naor, A. Shamir, in: M. Lomas (Ed.), Visual Cryptography, II: Improving the Contrast via the Cover Base,Presented at Security in Communication Networks, AmalE, Italy, September 16–17, 1996. Lecture Notes in Computer Science, Vol. 1189, Springer, Berlin, 1997.

3. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," vol. 250.

4. R. A. Ulichney, "The void-and-cluster method for dither array generation," in Proc. SPIE, Human Vision, Visual Processing, Digital Displays IV, Sep. 1996, vol. 1913.

5. Y. C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999.

6. Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain, Sept 2003, Vol. 1.