Multi Pixel Visual Cryptography for Colour Images in Meaningful Shares

Baby D Dayana [1], Jitesh Akaveeti [2], Kotha Karthik [3], M Sushmitha [4]
[1, 2, 3, 4] Department of Computer Science Engineering, SRM Institute of Science & Technology, Chennai, India

Abstract – Visual Cryptography is an encryption method to hide secret information in images so that when decrypted by using a correct key image secret information gets revealed. Visual Cryptography uses two transparent images. One of the images has random pixels while the other has secret information stored in it. Retrieval of the secret information from one specific image is impossible. Both transparent images/layers are required to reveal the information. Using the properties of the human visual system to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography. Encryption is done using simple algorithm which generates n copies of shares depending on the type of access structure schemes.

1. INTRODUCTION

Image confidentiality is assumed to be an important aspect in the daily routine. Programmed frameworks are favoured over any other.A programmed enigma/encryption can be used to achieve the confidentiality that is to be needed. It can be only possible by using an encryption method stated to be visual cryptography as it is done to images. Various algorithms are made for visual cryptography because of which confidentiality is spared to some degree. In the recent evolution of the digitization images are considered to be an important role in every human life and their confidentiality and clarity plays an important aspect for the image. The examination work demonstrates a programmed work for image secrecy/confidentiality as well as the image clarity . The required image is obtained b the decryption process. When the image is retrieved the pixel clarity tends to reduce eventually, which can be a major aspect for an image to be understood. This encryption process even helps in the safe retrieval of the image with its confidentiality intent while the image clarity is not disturbed.

At the encryption process the image gets divided into various parts depending on the algorithm which when necessarily combined gives us the required image necessarily. Those divided parts are meant to be known as shares in which some of them are not necessary and reduces the image pixel clarity. This visual cryptography process ignores the meaningless shares(shares that reduce the image clarity after decryption) and includes the meaningful ones(shares that provide necessary image when decrypted) . Toward the starting period , the image encryption was much of a problem and there were various security methods taken place to keep the image confidentiality intent. While, these days the digitized strategy is to provide security of the image has been a major development factor in the industry . The strategy mainly includes concepts of a couple of algorithms combined as shown in the System architecture .

Main asset of this process is Water Marking Algorithm based on which the encryption process can be made possible . The image is filtered in the first place to increase the clarity of the image by using necessary filters required. Then the specific image is decomposed into shares necessary, which undergo half toning process respectively. The digital images decomposed are then encoded accordingly based on the state of their decomposition after which the decomposed images are combined , which are possibly converted into shares accordingly by a random pixel selection-arrangement format where random pixels form respective n images/shares which doesn't make any sense until combined and decrypted, where the pixels necessarily are encrypted. The shares are then watermarked by using the water marking algorithm which is responsible for getting the secret/confidential image required by generating meaningful shares. The shares that are watermarked are then retrieved by the user whenever the user/ owner requires them for a purpose. The images are then decrypted by a sequential process of decryption known as staking . After the process is completed to the extent secret encrypted image is obtained in the final stage . the quality/clarity of the retrieved image doesn't differ in clarity from the original image.

2. SYSTEM ARCHITECTURE

a) Filters:

The filters for encoding are required to eliminate the noise and to sharpen the secret input image. Types of filters include:

- *Laplacian filter*:

It sharpens the image for better recovered result.

- *Low pass average filter*:

It filters the image and blurs the gaussian noise.

- *Min and Max filters*:

It is used to eliminate pepper and salt noises.

b) Decomposition:

Three channels C, M and Y are the three channels used to decompose the input image.The Cyan , Magenta and yellow colours are not shown on the screen as MATLAB does not support it along with the monitor. On the monitor it looks as a grey scale image.As MATLAb cannot display the CMY images directly, it is printed in TIFF format with array size[mxnx4]

c) Halftoning:

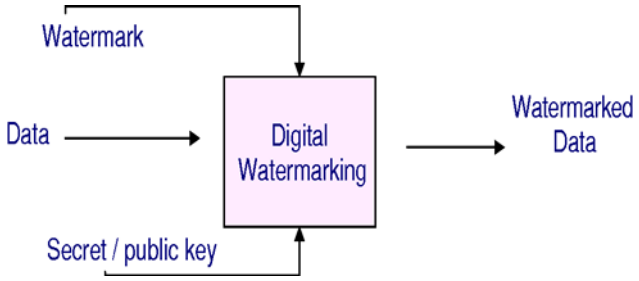
A reprographic technique which simulates continuous tone imagery by the use of dots and generates gradient effect. High quality halftones are by produced by error diffusion. Every monochrome image has halftone applied on it which is treated as a gray-scale image and converted to binary. The image is scanned from left to right or from top to bottom

d) Encryption:

Encryption process generates shares when it is applied on each halftone channel. Each halftone has two shares C – C1 & C2, M – M1 & M2, Y – Y1 & Y2.

e) Watermarking:

Watermarking hides the digital information in a carrier signal and also verify the authenticity and integrity of the carrier signal. It is covertly embedded in a voice- tolerant signal(secret image).



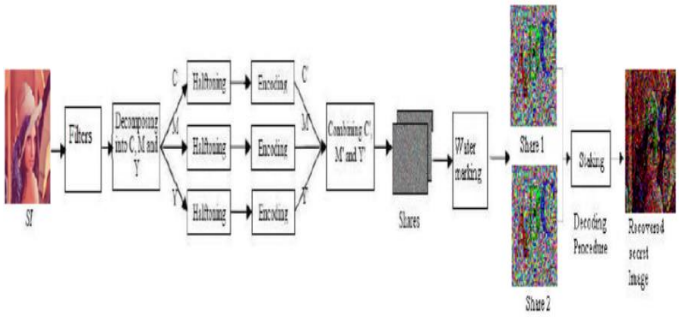
3. EXISTING SYSTEM

Images are manipulated by the attackers in the network. Confidential Images has no means to be secured when they are transmitted over the network.

In general visual cryptography methods, only a piece of image gets encoded in the encryption process. And each of the shares that are generated was shown as a disorganized image, and they are easily suspected by hacker. The generated shares are not meaningful.

4. PROPOSED SYSTEM

In the proposed scheme two meaningful shares are generated for color images. Better filters are used for improving the quality of the retrieved image. The considered secret image is decomposed into three channels named C ,M & Y(Cyan, Magenta and Yellow) by the usage of an equation. Halftone of much higher quality is produced through error diffusion. Halftone is applied on each monochrome image and on each halftone channel for generating shares. There will be two shares for each halftone. A multi-pixel scheme for color images which can encode more than one pixel for every run that results in same size of shares as the secret image. Advanced watermarking algorithm is proposed to generate meaningful shares. Decryption is achieved by stacking the shares. In case of black pixel, overlaying two rows of M1 results in four black bits, and reveals the information, whereas for the white pixel, stacking the two rows of M0 produces two black and two white bits, and introduces noise.



5. CONCLUSION AND FUTURE SCOPE

The proposed system is made to implement a mechanism to improve the quality of recovered image in visual cryptography using meaningful shares.The framework uses a Laplacian filter, min-max filter, average filter, watermarking method , halftone encryption method uses only meaningful shares for the better quality of the secret image. Before watermarking shares are random dots which do not reveal the secret information. Shares are watermarked using watermarking algorithm which without revealing the secret information gives meaningful shares which can be revealed by overlapping of the meaningful shares.

REFERENCES

[1] M. Naor and A. Shamir, Visual cryptography, Advances in Cryptology EUROCRYPT ’94, Lecture Notes in Computer Science, vol.950, no.7, pp.1–12, 1995.

[2] Debasish Jena and Sanjay Kumar Jena, A Novel Visual Cryptography Scheme, International Conference on Digital Object Identifier, pp.207 – 211, 2008.

[3] Hsien-Chu Wu, Hao-Cheng Wang and Rui-Wen Yu, Color visual Cryptography Scheme using Meaningful Shares, Eighth International Conference on Digital Object Identifier, Volume 3, pp.173 – 178, 2008.

[4] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, Visual Cryptography for General Access Structure by Multi-pixel Encoding with Variable Block Size, International Symposium on Digital Object Identifier, pp.340 – 344,2008.

[5] Zhongmin Wang and Gonzalo R. Arce, Halftone visual cryptography through error diffusion, IEEE Transactions on Digital Object Identifier, Volume 4, Issue 3, pp.109-112, 2006