ISSN:2320-0790

An International Journal of Advanced Computer Technology

Review of Digital Image Sharing By Diverse Image Media

[1]MAYURI SONKUSARE, [2]PROF. NITIN JANWE

[1,2]Computer Science and Engineering Department

Abstract: A natural-image-based VSS scheme (NVSS scheme) that shares secret images. A natural-image-based secret image sharing scheme (NSISS) that can share a color secret image over n - 1 arbitrary natural images and one noise-like share image. Instead of altering the contents of the natural images, the encryption process extracts feature images from each natural image. In order to protect the secret image from transmission phase. (n, n) - NVSS scheme shared secret image over n-1 natural share. The natural shares will be digital image and printed image. By extracting the features of natural shares we can prepare noise-like share. After that encryption carried out with noise-like share and secret image. Propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. In this paper Initially Feature Extraction process has been performed for Natural Shares. Here Digital image and Printed image have been used as Natural Shares. With that extracted features secret image will be encrypted by (n, n) - NVSS scheme where process carried by (n-1) natural shares. This Encrypted result will be hided using Share-Hiding Algorithm where generated the QR code. In the Recovering of the secret image will be done by Share Extraction Algorithm and also decryption algorithm. Finally the secret image with all pixels has been obtained. This proposed possible ways to hide the noise like share to reduce the transmission risk problem for the share.

Keywords: **Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk.**

1. INTRODUCTION

Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images.a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data.

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. As a result, different security techniques have been used to provide the required protection. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

Introduction to Image Processing

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows.

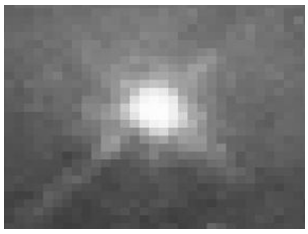


Figure 1: An image — an array or a matrix of pixels arranged in columns and rows.

In a (8-bit) greyscale image each picture element has an assigned intensity that ranges from 0 to 255. A grey scale image is what people normally call a black and white image, but the name emphasizes that such an image will also include many shades of grey.

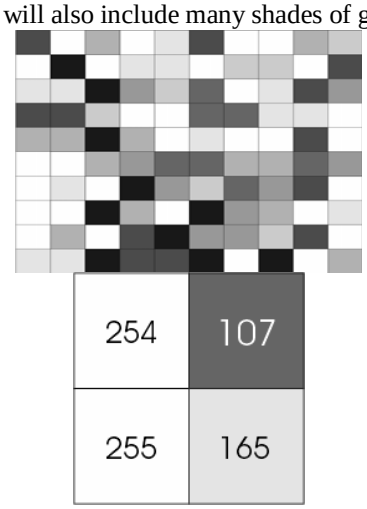


Figure 2: Each pixel has a value from 0 (black) to 255 (white).

A normal greyscale image has 8 bit colour depth = 256 greyscales. A "true colour" image has 24 bit colour depth = 8 x 8 x 8 bits = 256 x 256 x 256 colours = ~16 million colours.

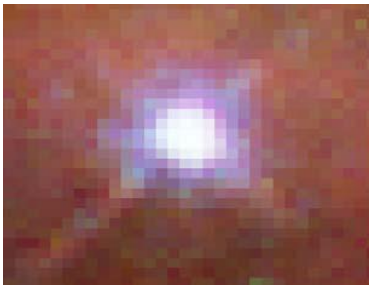


Figure 3: A true-colour image assembled from three greyscale images coloured red, green and blue. Such an image may contain up to 16 million different colours.

Some greyscale images have more greyscales, for instance 16 bit = 65536 greyscales.

There are two general groups of 'images': vector graphics (or line art) and bitmaps (pixel-based or 'images'). Pictures concisely convey information about positions, sizes and inter relationships between objects. Human beings are good at deriving information from such images, because of our innate visual and mental abilities. An image is digitized to convert it to a form which can be stored in a computer's memory or on some form of storage media such as a hard disk or CD-ROM. This digitization procedure can be done by a scanner, or by a video camera connected to a frame grabber board in a computer.

Image processing operations can be roughly divided into three major categories, Image Compression, Image Enhancement and Restoration, and Measurement Extraction. It involves reducing the amount of memory needed to store a digital image. Image defects which could be caused by the digitization process or by faults in the imaging set-up (for example, bad lighting) can be corrected using Image Enhancement techniques. Once the image is in good condition, the Measurement Extraction operations can be used to obtain useful information from the image.

Images and digital images

Suppose we take an image, a photo, say. For the moment, lets make things easy and suppose the photo is black and white (that is, lots of shades of grey), so no color. We may consider this image as being a two dimensional function, where the function values give the brightness of the image at any given point. We may assume that in such an image brightness values can be any real numbers in the range (black) (white).

A digital image from a photo in that the values are all discrete. Usually they take on only integer values. The brightness values also ranging from 0 (black) to 255 (white). A digital image can be considered as a large array of discrete dots, each of which has a brightness associated with it. These dots are called picture elements, or more simply pixels. The pixels surrounding a given pixel constitute its neighborhood.

Some applications:

Image processing has an enormous range of applications; almost every area of science and technology can make use of image processing methods.

1. Medicine

- Inspection and interpretation of images obtained from X-rays, MRI or CAT scans,
- analysis of cell images, of chromosome karyotypes.

2. Industry

- Automatic inspection of items on a production line,
- inspection of paper samples.

Digital Image Processing

Image Processing Toolbox™ provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration. Many toolbox functions support multicore processors, GPUs, and C-code generation. Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Visualization functions and apps let you explore

images and videos, examine a region of pixels, adjust color and contrast, create contours or histograms, and manipulate regions of interest (ROIs). The toolbox supports workflows for processing, displaying, and navigating large images.

Image Preprocessing

The probabilistic models attempt to characterize the key properties of an image, basedon which imaging problem can be described, formulated and resolved. For example, the goal of image restoration is to enhance and to improve the appearance of an image by estimatingthe original pixel values from the distorted observation.

Image Encryption

In cryptography, encryption is the process of encoding messages (or information) in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded.

2. IMAGE PROCESSING FUNDAMENTALS

Pixel: In order for any digital computer processing to be carried out on an image, it must first be stored within the computer in a suitable form that can be manipulated by a computer program. The most practical way of doing this is to divide the image up into a collection of discrete (and usually small) cells, which are known as *pixels*. Most commonly, the image is divided up into a rectangular grid of pixels, so that each pixel is itself a small rectangle. Once this has been done, each pixel is given a pixel value that represents the color of that pixel. It is assumed that the whole pixel is the same color, and so any color variation that did exist within the area of the pixel before the image was discretized is lost. However, if the area of each pixel is very small, then the discrete nature of the image is often not visible to the human eye.

Other pixel shapes and formations can be used, most notably the hexagonal grid, in which each pixel is a small hexagon. This has some advantages in image processing, including the fact that pixel connectivity is less ambiguously defined than with a square grid, but hexagonal grids are not widely used.

Pixel Connectivity

The notation of pixel connectivity describes a relation between two or more pixels. For two pixels to be connected they have to fulfill certain conditions on the pixel brightness and spatial adjacency.

First, in order for two pixels to be considered connected, their pixel values must both be from the same set of values *V*. For a grayscale image, *V* might be any range of graylevels, *e.g.V={22,23,...40}*, for a binary image we simple have *V={1}*. To formulate the adjacency criterion for connectivity, we first introduce the notation of *neighborhood*. For a pixel *p* with the coordinates *(x,y)* the set of pixels given by:

$$N_4(p) = \{(x+1, y), (x-1, y), (x, y+1), (x, y-1)\}$$

is called its *4-neighbors*. Its *8-neighbors* are defined as

$$N_8(p) = N_4 \cup \{(x+1, y+1), (x+1, y-1), (x-1, y+1), (x-1, y-1)\}$$

From this we can infer the definition for *4*- and *8-connectivity*:

Two pixels *p* and *q*, both having values from a set *V* are *4*-connected if *q* is from the set $N_4(p)$ and *8*-connected if *q* is from $N_8(p)$. General connectivity can either be based on *4*- or *8*-connectivity; for the following discussion we use *4*-connectivity. A pixel *p* is connected to a pixel *q* if *p* is *4*-connected to *q* or if *p* is *4*-connected to a third pixel which itself is connected to *q*. Or, in other words, two pixels *q* and *p* are connected if there is a path from *p* and *q* on which each pixel is *4*-connected to the next one. A set of pixels in an image which are all *connected* to each other is called a *connected component*. Finding all connected components in an image and marking each of them with a distinctive label is called connected component labeling. An example of a binary image with two connected components which are based on *4*-connectivity can be seen in Figure 1. If the connectivity were based on *8*-neighbors, the two connected components would merge into one.

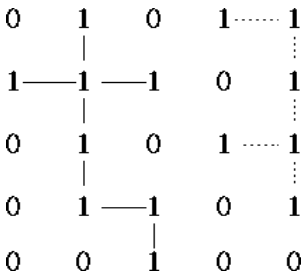


Figure 1 Two connected components based on *4*-connectivity.

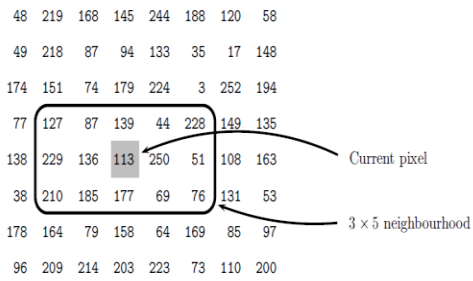
Pixel Values

Each of the pixels that represents an image stored inside a computer has a *pixel value* which describes how bright that pixel is, and/or what color it should be. In the simplest case of binary images , the pixel value is a 1-bit number indicating either foreground or background. For a gray scale images, the pixel

value is a single number that represents the brightness of the pixel. The most common *pixel format* is the *byte image*, where this number is stored as an 8-bit integer giving a range of possible values from 0 to 255. Typically zero is taken to be black, and 255 is taken to be white. Values in between make up the different shades of gray.

To represent color images , separate red, green and blue components must be specified for each pixel (assuming an RGB color space), and so the pixel `value' is actually a vector of three numbers. Often the three different components are stored as three separate `grayscale' images known as *color planes* (one for each of red, green and blue), which have to be recombined when displaying or processing. Multispectral Images can contain even more than three components for each pixel, and by extension these are stored in the same kind of way, as a vector pixel value, or as separate color planes. The actual grayscale or color component intensities for each pixel may not actually be stored explicitly. Although simple 8-bit integers or vectors of 8-bit integers are the most common sorts of pixel values used, some image formats support different types of value, for instance 32-bit signed integers or floating point values. Such values are extremely useful in image processing as they allow processing to be carried out on the image where the resulting pixel values are not necessarily 8-bit integers. If this approach is used then it is usually necessary to set up a color map which relates particular ranges of pixel values to particular displayed colors.

Pixels, with a neighborhood:



Color scale

The two main color spaces are **RGB** and **CMYK.**

RGB

The **RGB color model** is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. RGB uses additive color mixing and is the basic color model used in television or any other medium that projects color with light. It is the basic color model used in computers and for web graphics, but it cannot be used for print production. The secondary colors of RGB – cyan, magenta, and yellow – are formed by mixing two of the primary colors (**red, green** or **blue**) and excluding the third color. Red and green combine to make yellow, green and blue to make cyan, and blue and red form magenta. The combination of red, green, and blue in full intensity makes white.[figure4]

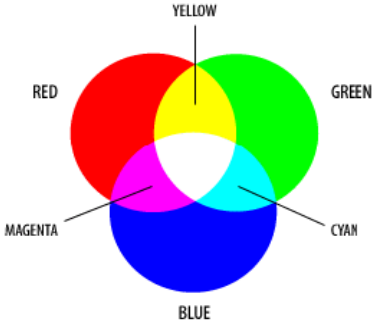
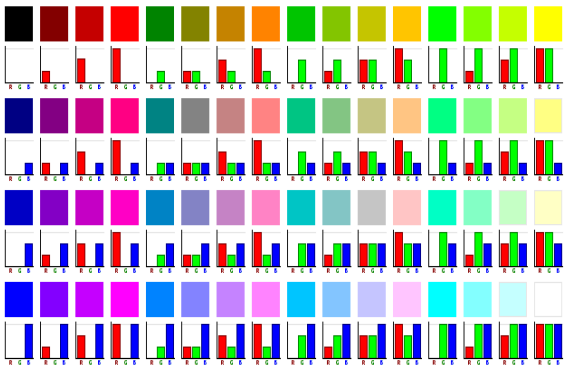


Figure [4]: The additive model of RGB. Red, green, and blue are the primary stimuli for human color perception and are the primary additive colors.

To see how different RGB components combine together, here is a selected repertoire of colors and their respective relative intensities for each of the red, green, and blue components:



Some applications:

Image processing has an enormous range of applications; almost every area of science and technology can make use of image processing methods.

1. Medicine

- Inspection and interpretation of images obtained from X-rays, MRI or CAT scans,
- analysis of cell images, of chromosome karyotypes.

2. Industry

- Automatic inspection of items on a production line,
- inspection of paper samples.

Process with image using techniques:

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame. The output of image processing may be either an image or a set of characteristics or

parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. Image processing is closely related to computer graphics and computer vision. Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image.

Digital Image Processing

Image Processing Toolbox™ provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration. Many toolbox functions support multicore processors, GPUs, and C-code generation. Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Visualization functions and apps let you explore images and videos, examine a region of pixels, adjust color and contrast, create contours or histograms, and manipulate regions of interest (ROIs). The toolbox supports workflows for processing, displaying, and navigating large images.

Image Preprocessing

The probabilistic models attempt to characterize the key properties of an image, basedon which imaging problem can be described, formulated and resolved. For example, the goal of image restoration is to enhance and to improve the appearance of an image by estimatingthe original pixel values from the distorted observation. Due to high-dimensionality in spatial interactions, however, modeling the statistics of images is a challenging task. The first step in reducing dimensionality is tomake some simplifying assumptions regarding the pixel interrelationships. A new form of minimization functional for solving image inverse problem is formulated using JSM under regularization-based framework. Extensive experiments on image inpainting, image deblurring and mixed Gaussian plus salt-and-pepper noise removal applications verify the effectiveness of the proposed algorithm.

Image Encryption

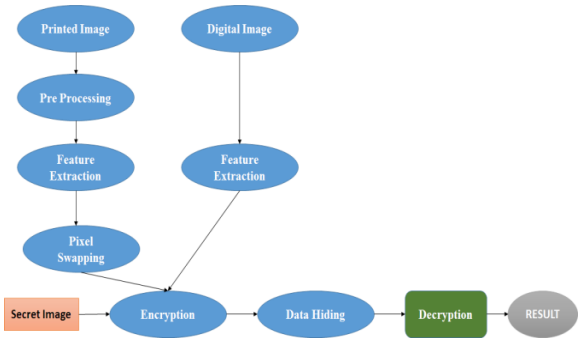
In cryptography, encryption is the process of encoding messages (or information) in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message

3. RESULTS AND DISCUSSION

In our proposed system (n, n) - NVSS scheme has been implemented. Here both printed image and digital image have been taken into account to create the noise-like share. This natural image needed to be extracted feature for further process. With the featured image and secret image can perform encryption process. By applying (n, n) NVSS scheme developed encrypted image or (n-1) natural share.

Feature extraction has been performed for two natural shares, so as the natural share's pixels are more efficiently compressed. These extracted features are encrypted with Secret Image. This process is performed by (n, n) - NVSS scheme. Then the encrypted image will be hided using share hiding algorithm. This process performed with the QR code technology. QR code is a two-dimensional code. The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. The transmission risk of the conventional VSS schemes increases rapidly. On the contrary, regardless of the increasing number of shares, the proposed NVSS scheme always requires only one generated share. In decryption process Share extraction algorithm performed and decryption algorithm applied to recover the Secret image.

Block Diagram:



Advantage:

- In order to implement the natural share by feature extraction and pixel swapping can effectively improve the performance of encryption process.
- To combine the QR code in the step of Data Hiding can make it suitable for use as a carrier of secret communications.

CONCLUSIONS

In this paper a VSS scheme, (n, n)-NVSS scheme, that can share a digital image using diverse image media. The media that include n-1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants n increases, the NVSS scheme uses only one noise share for sharing the secret image.It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share, however, it can recognize the colorful secret messages having even low contrast.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia,"Incrementing visual cryptography using random grids," Opt. Commun., vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[3] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[4] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.

[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[6] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," Int. J. Pattern Recognit. Artif.Intell., vol. 21, no. 5, pp. 879–898, Aug. 2007.

[7] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[10] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.

[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes,"IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[12] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

[13] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images," Digit. Signal Process., vol. 21, no. 6, pp. 734–745, Dec. 2011.