International Journal of Scientific Research and Modern Education (IJSRME)
Impact Factor: 7.137, ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume 5, Issue 1, 2020

NATURAL IMAGE VISUAL SECRET BY DIGITAL IMAGE SHARE

Dr. A. Rosi*, W. Mesiya Stalin & C. Sudhakar*****
Assistant Professor, Department of Electronics and Communication Engineering,
Dhanalakshmi Srinivasan Institute of Technology, Samayapuram, Trichy, Tamilnadu

Cite This Article: Dr. A. Rosi, W. Mesiya Stalin & C. Sudhakar, "Natural Image Visual Secret by Digital Image Share", International Journal of Scientific Research and Modern Education, Volume 5, Issue 1, Page Number 1-3, 2020.

Abstract:

Visual information like picture, text is encrypted by visual cryptography. Basically cryptography is used to hiding data in pictures. These encrypted images can be decrypt by human vision by the decrypt key. A typical visual secret sharing (VSS) method conceals confidential images into multiple parts, where images are saved as digital images and encrypted. Different part of images can appear as noisy images. But these images will prompt some distrust questions and increase obstruct danger situation during communication of n images. Therefore, visual secret sharing methods got more miserable communication issues for both member and confidential images. To resolve this issue, this paper provides a solution as a Natural image Visual Secret Sharing method (NVSS). It distributes the confidential pictures through different channels to secure the confidential images during the communication section. Digital or printed form of confidential digital image and noisy images are shared by proposed NVSS**.** Depends on the natural shares and the secret image the noisy images were generated. The original images are used to reducing the communication issues.

Key Words: Cryptography, Natural image, Encryption, Decryption & QRCODE

Introduction:

The core objective of this paper is to prevent the communication issues to share an image in a network. Recovered image will be formed after decryption process has been done. A recovered image doesn't have any pixel expansion and pixel corruption. In this process the Secret image and recovered image doesn't change anymore.

User Classes and Characteristics:

The QR code is 2D code which is developed for automotive industry. A QR code encrypts the information in vertical and horizontal directions [6]. Compare with barcode, QR code can hold huge size of data. The main advantage of this QR code is it can be print on any physical devices and it can be read and decoded by barcode readers and smart phones [6]. Nowadays QR code is used in all products like electronic devices, catalogs, appliances commercial and residential products etc… The main purpose of the QR code is secret communications.

Constraints in Implementation:

Hierarchical structures of relations are very complicate implement which may result in more classes. So hierarchical structure is transform to a simpler structure. This is used to transform the hierarchical model into a bipartite, flat model[4]. A flat relation doesn't have any identity and it is used at the design level of simplicity and implementation. Entity-relationship model and object oriented methods are similar to the flat relation.

Related Work:

Visual cryptography method is used to split up the confidential image into n number of images, which is known as n shares. These n numbers of images are shared via some private or public network. While sharing this multiple images many unauthorized user can try to corrupt these images. If any image can be corrupted by any unofficial person, then the receiver couldn't configure the right image. If the receiver finds that any of the shared images is not corrupted by unauthorized user, they have to merge the n images to get the recovered or original image [2]. At the same time the recovered images have some noisy look. So the recovered image has some poor clarity, poor display and pixel expansion. With the use of these images (recovered image, pixel expansion images) researches have done a big business.

Literature Survey:

Hiding the information or data in image is an early technique. Using this technique we can send the secret image to someone. This technique is called Conventional Visual Secret Sharing. But this technique has built with good encryption algorithm with advanced structure. But it has lot of disadvantages during transmission. Hackers can track the information, poor clarity, lack of data loss, etc.... To overcome these issues, Udmale et.al had proposed natural image based visual secret sharing technique introduced [6]. The NVSS method is used for regeneration of secret at the receiver's end. So generate the new noisy image is important to hide the data in another image. So this NVSS technique improves efficiency using block wise rotation. Peak Signal to Noise Ratio is used to check the performance by time [6].

To hide confidential images in share we have used conventional visual secret sharing technique. The n number of images can be materializing as noisy pixels or as meaningful images. To overcome this issue Lee et.

al had proposed a Natural Imaged Visual Secret Sharing technique that shares secret images through different channels to save secret images during communication section. This technique shares one secret image which is in digital form over n-1 arbitrary [3]. This n-1 arbitrary is called natural images. The natural image is a digital form of photos or painted pictures. Depends on the natural image and secret image the noisy images were generated. Unmodified natural images are used to reduce the communication issues [3].

A new Natural Image Visual Secret Sharing technique was introduced. Using this n-1 natural image and one noisy image we can share a secret image. It doesn't affect or disturb the data of natural images. Features of natural image and secret images are extracts by using encryption algorithm and converted to multiple images or n number of images. This technique is used to reduce the communication and management issues. In this proposed system Rao yet.al. had proposed steganography is included to NVSS scheme to securely transfer data by hiding it behind the secret image. Steganography is the additional security element added with NVSS for transfer the images [4]. Then the final secret images are in encrypted format. This secret image is converted into multiple images. This steganography technique is applicable for black and white images, grey scale images and color images also [4].

Proposed System:

The natural n images could be black and white images or color images and it should be in digital or printed form. Features of natural n images can be extracted by the encryption process. This encryption process doesn't change the natural n images. The secret image is generating the n number of images, and its features are extracted from natural shares. This paper provides a solution as a natural image visual secret sharing method that distributes the confidential pictures through different channels to secure the confidential images during the communication section Digital or printed form of confidential digital image and noisy images are shared by proposed NVSS**.** Depends on the natural shares and the secret image the noisy images were generated. The original images are used to reducing the communication issues. Extraction and encryption is the two important features in NVSS. Using a XOR operation the secret image generates one noisy image. To get the recovered image, the decryption method and extracts features from all natural n number of images execute the XOR operation.

Image Selection and Image Preparation:

At the first natural pictures and secret pictures are chosen. Natural images are colored as digital images. Digital images are extracted from the printed image. Process of image generation is used for printed preprocess images and feature matrices post process images. The following process of image preparation is

- Electronic devices like digital cameras, smart phones, digital scanners and some mobile and desktop applications may acquire the information of printed images.
- At the last printed images are modified or cropped, so both natural and printed images are have same dimensions.

Feature Extraction and Encryption Process:

This extraction and encryption process is used to extracts the feature images from the natural images. This extraction and encryption process is the core process and concurrently it is appropriate to printed and digital images. So consider the magnitude of confidential image and natural image**.** The following notations are defining the above process. Block size is represents as b.

QRCODE Generation and Network Sharing Process:

Basically, QRCODE technology is developed for hide noisy images and used to reduce intercepted risk issues while image sharing can be done. Encrypted images are fixing into binary numbers. It is not possible to embed all the binary numbers to QRCODE. Finite number of binary numbers would be fixing into QRCODE. Because of this issue, all binary numbers are separated into multiple parts. These separated binary numbers and respective keys are stored in a collection framework. From the collection framework, binary numbers are extracted using this key act and it extracted and fixing to the QRCODE once we stored the entire separated binary numbers once the QRCODE has been formed. Sender sends the natural n numbers of images, collection framework and QRCODE. If the receiver is authorized, they can access and receive the images. At the same time if the receiver is not authorized they won't receive any images.

Encryption and Decryption process of Image Extraction:

Once receiver get all those images, by using QRCODE reader application in smart phones image has to scan the QRCODE. Receiver will get all keys for divided binary values once the scanning process can be done. After that key values should be sending to the receiver application by socket communication. Encrypted images are formed by collection framework and receiver extract the binary numbers using these keys. Once encrypted images are reached receiver like Encryption, decryption process also has been done.

Conclusion:

This paper proposes a new technique called VSS method and NVSS method. It can be used to share the digital image using diverse media. This media have multiple images, which are randomly chosen and unmodified in encryption section. While sharing the secret image the NVSS method uses only one noise. The proposed NVSS method is better than existing VSS method in reduce image communication issues and it is consider as user friendly for both n number of images and sender and receiver. This paper provides four major contributions. The images are shared through heterogeneous carriers in a VSS method for a first time. We successfully introduce hand-printed images for images-haring methods. This paper proposes a useful concept and method for using unmodified images as shares in a VSS method. We develop a method to store the noise share as the QR code [6].

References:

1. L. J. Anbarasi, M. J. Vincent and G. S. A. Mala, "A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography," 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, 2011, pp. 129-133.
2. I. Kang, G. R. Arce and H. K. Lee, "Color Extended Visual Cryptography Using Error Diffusion," in IEEE Transactions on Image Processing, vol. 20, no. 1, pp. 132-145, Jan. 2011.
3. K. H. Lee and P. L. Chiu, "Digital Image Sharing by Diverse Image Media," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 88-98, Jan. 2014.
4. J. Rao and S. Patel, "A novel approach for enhancing image security and data hiding using NVSS," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 1128-1133.
5. N. Sharma, A. Goyal and A. Suryavanshi, "Improved NVSS scheme for diverse image media," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 2014, pp. 1515-1521.
6. A. M. Udmale and S. B. Nimbekar, "Efficient block wise data hiding for securely digital image sharing by diverse image media," 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, 2016, pp. 133-137.