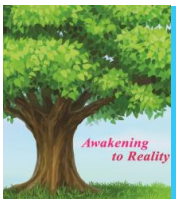

Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 116 (2018) 50136-50140

Elixir
ISSN: 2229-712X

Enhancing Image Security and Data Hiding Using NVSS

T. Narendrababu, V.V.S.Sireesha, N.Divya Teja,Y.Komali and S.Uma Maheswar Reddy
Department of CSE, Tirumala Engineering College.

ARTICLE INFO

Article history:
Received: 12 February 2018;
Received in revised form:
8 March 2018;
Accepted: 20 March 2018;

Keywords
Data Hiding,
Natural Images,
Transmission Risk,
Visual Secret Sharing.

ABSTRACT
Visual Secret sharing (VSS) suffer from secret transmission risk as the shares in VSS appear as meaningful image or noise like image. In order to overcome such problem a new Natural image based Visual Secret Sharing (NVSS) scheme was presented. Using NVSS scheme one can distribute a secret image using n-1 natural images and one noise image. It does not modify the contents of natural images. The encryption phase extracts features of every natural image. The secret image is converted to a share by performing computations on secret image and feature extracted from natural images. On the other hand the secret image is retrieved by performing computations on the share and the feature extracted from natural images. This scheme can be used to decrease the risk of transmission and also resolve the management problems. In our proposed system steganography is included to NVSS scheme to securely transfer data by hiding it behind the secret image. To increase the security further this secret data is encrypted before performing steganography. Hence the secret data is in encrypted format. This secret image is then converted into share which is finally embedded in cover image. This proposed scheme is able to share black and white, grey level or color images secretly. Also this scheme is easy to implement.

© 2018 Elixir All rights reserved.

I. INTRODUCTION

Modern world has become almost digitalized touching every field like education, government sectors, industrial sectors, commerce etc. Today, most of the transactions are carried over internet. This involves huge risk as many hackers or attackers are present on the internet. These hackers hack the private or confidential information being transmitted over internet to misuse it. This provides biggest threat to the user. To provide security to this data being transmitted over internet cryptography is used. Cryptography is a technique that converts the plain text data into unreadable format known as cipher text using some cryptographic algorithm. This is then transmitted over internet so that the hacker cannot reveal the data. At the receiver end the cipher text is deciphered to obtain the original plain text data.

Visual cryptography (VC) is a method that converts secret image into n number of shares [1]. These shares are then distributed to the participants who are involved in it. Anyone who has shares less than n shares cannot retrieve any information regarding the secret image. This secret image can be retrieved only after overlapping n shares. VC is very simple technique because it uses the human visual system to decrypt the secret image. Visual secret sharing (VSS) is a process to share and deliver secret images [9]. VC has some limitations:

1) VC involves great transmission risk as the noise-like shares will arouse doubt to attackers. Hence the shares might be intercepted.
2) Also, the shares which are meaningless are not user-friendly. The difficulty in managing shares rises with the increase in number of shares.

NVSS stands for Natural Image based Visual Secret Sharing scheme [5].

This scheme reduces possibility of intercepting shares while it is being transmitted. Earlier VSS schemes made use of unity carrier which may be either digital images or transparencies for image sharing. This is the main limitation of VSS schemes. Using NVSS scheme, it has become possible to use different medium to share images. The medium used as carrier in this technique can be the image which may be in printed form, or digital form, etc. Using diverse medium to share secret image lessens the probability of intercepting the shares.For increasing the security further steganography is applied. Many attackers are present who can hack the secret image during its transmission. Therefore, image steganography has become extremely important to preserve the privacy of image transmitted over internet. Steganography involves hiding of information. In steganography only the sender and receiver is aware that some information is hidden. Cryptography is used only for securing the message whereas, steganography is involves hiding the presence of secret message. In this paper the secret message is first encrypted by using cryptography to obtain cipher text. This cipher text is hidden behind the secret image by using steganography and finally the secret image is XORed with the feature images obtained from natural image pre-processing stage to obtain share. This share is embedded behind cover image. This cover image embedded with share is then transmitted to receiver over the network where the receiver performs decryption process to extract secret image from the cover image and ciphered secret data from the secret image. Then the data is deciphered to obtain the original data.

Related work is presented in Section II. Section III explains the proposed system. Section IV shows expected result and Section V concludes the paper.

Tele:
E-mail address: tnarendrababu@gmail.com

© 2018 Elixir All rights reserved

II. RELATED WORK

Moni Naor and Adi Shamir presented a Visual Secret Sharing technique which was termed as (k, n) secret sharing problem. They made assumptions that the image consists of B&W pixels where every pixel is controlled independently. The white pixel signifies the transparent color. The drawback is that the deciphering process results in loss of contrast [1].

Zhou et al. presented halftone visual cryptography technique for performing VC via halftoning. In order to encrypt the binary secret image into n halftone image that is intended to contain some important visual information, this method uses void and cluster algorithm [10]. The result of simulation reveals that the generated halftone shares have better visual quality [2].

A novel hiding method was proposed for 2 halftone secret images converted into two meaningful shares which are generated using the halftone cover image. These meaningful image shares are appropriate as compared to the meaningless shares containing noise in the VSS scheme as they appear like natural images and do not take attention of eavesdroppers. Existing works in such scheme emphasize on containing more secrets and generating meaningful image shares for a single secret image. Such methodology increases the amount of secrets and also generates meaningful image shares simultaneously. Even the contrast of image shares is same as Extended VC schemes. In such schemes two secrets in the images are encrypted into two shares. One of the two images which appear like natural image may be used as cover of image apart from the Halftone VC method where one of the cover which must be opposite from that of the other image cover and which can encrypt one secret in image. The presented algorithm can be further extended to be applicable for sharing color images using halftone technique, color composition and color decomposition. Specifically, error diffusion algorithm is followed for color images [3].

A new color VCS that is based on the modified VC can share secret images such as a color secret image using different natural images and one noise-containing share image. This scheme does not alter the features of natural images. Here, the encrypting process removes the features from every natural image. This is how the proposed scheme can efficiently decrease the risk of transmission and also overcome the problem of managing shares. Using this problem of pixel expansion is removed. It also creates the ease to regenerate secret images having high contrast. Due to this, the suggested scheme can share black & white pixels, gray-level VC or color images VC in secret manner [4].

The (n, n) NVSS scheme enables us to share a secret image in digital form image using n - 1 different natural images and one noise-like share. The natural image may be in any format like printed, digital etc. The natural shares are not altered. These natural shares and the secret image are used to produce the noise-like share. These shares are different and natural, therefore it decreases the risk related with transmission. They also proposed some technique to hide the noise-like share for securing its transmission. They carried out experiment and revealed that their presented approach is the best way to solve the problem of transmission in VSS [5].

The extension to the previous VSS was given by presenting (2, 2) VSS scheme without causing size expansion. This approach aims to encrypt a secret block having four pixels into two shares based on the distribution of B&W pixels. This can permit the restoring of secret image with XOR operation. This technique is applicable to binary as well as halftone images. It does not cause pixel expansion [6].

A method to report many issues without the requirement of codebook design was also presented. Such method is applicable to binary secret images with decryption environments which is non-computer based. For avoiding pixel expansion, the authors have developed a set of column vectors for encryption of secret pixels. They carried out experiment and revealed that this scheme can achieve better contrast [7].

Sasaki et al. provided the formulation of VSS encryption for multiple secret. The restriction with EVCS Scheme was that each share had additional secret image associated with it. Even the restriction with VSS-q-PI was that multiple secret images are accompanied with the corresponding shares in qualified sets but the shares in forbidden sets must be similar. Therefore they presented a generalized VSS scheme for encrypting multiple secret images [8].

III. PROPOSED SYSTEM

This system is used for securely transferring secret data and secret image over network.

In the first step we select the secret data and secret image that is to be secured while transmission. The data which is to be sent secretly is hidden behind this secret image. Further to increase the security of data, the data is first encrypted using private key cryptographic technique before embedding with secret image. The data is converted to cipher text. The cipher text is not in readable format. Therefore, it cannot be intercepted by the attacker. Only sender and receiver know how to decrypt the cipher text. As a result the data is secured. In the steganography module the ciphered data is hidden behind the secret image. After performing steganography the secret image containing cipher data hidden behind it is converted into share with the help of feature extraction process and then embedded with the cover image. This image is transmitted through network. This image does not attract the attacker's attention. After receiving the image, the receiver performs decryption. The receiver separates the share from the cover image.

TABLE I. LIST OF SYMBOLS AND DESCRIPTION

Symbol	Description
PT	Plain Text
CT	Cipher Text
K	Private Key
ESI	Embedded Secret Image
E	Encryption
D	Decryption
SI	Secret Image
N	Natural Images
Np	Printed Image
Nd	Digital Image
S'	Share
F	Feature Image
B	Block size (even)
(x, y)	Coordinates of pixels
(x1,y1)	Coordinates of top-left pixels in a block
(xb, yb)	Coordinates of bottom-right pixels in a block
f(x, y)	Feature value of pixel (x, y)
p_φ^(x,y)	Value of color $\phi \epsilon$ (R,G,B) for pixel (x, y)
H^(x,y)	Sum of RGB color values of pixel (x, y) in N
T	Amount of pixel swapping for a feature image of a printed image
Qc	Candidate pixel

After performing computation with share and feature extracted from natural images the secret image is revealed.

Further the receiver extracts the ciphered data from the secret image. This ciphered data is deciphered using cryptographic technique to obtain original data. Thus the receiver gets both secret image as well as secret data. In this way, our proposed system secures image as well as data transmission.

A. Sender Side Architecture

The proposed sender side consists of four main modules such as Steganography module, Natural image processing module, Encryption module and Application of cover image module.

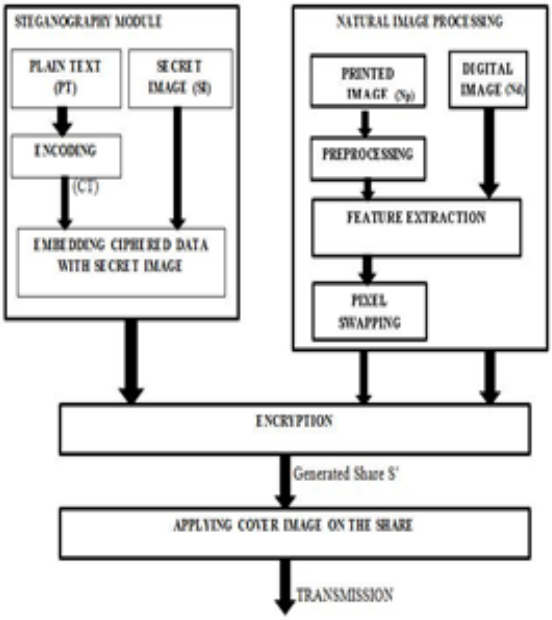

Fig. 1. Sender side block diagram.

1) Steganography Module

As shown in Fig. 1, this module consists of Plain text (PT) and secret image (SI). Secret data is in the form of plain text. The plain text is applied as an input to encoding phase where it is converted into cipher text (CT) using private key cryptography. This cipher text is finally embedded with the secret image so that the presence of text behind the image is unknown to others. This means that steganography is used because the attacker cannot guess the presence of some secret information behind image. Hence it can provide considerable security to the data hidden behind image.

Mathematically this can be represented as :

Step 1: CT ←E (PT, K)

Step 2: ESI←SI+CT

2) Natural Image Processing

This module is the core module which can use either digital or printed images. The printed image is pre-processed using image preparation and pixel-swapping.

Feature Extraction

This module performs feature extraction by extracting features from the natural shares which may be in the form of printed image (Np) or digital image (Nd). In this the natural shares are not modified. As there is no modification in the natural share, it will not seek the attackers' attention while transmission. In case, if the natural shares are captured, the attackers won't be able to figure out that there is some hidden information behind the image. Therefore, transmitting the innocent share is more secure than transmitting meaningful or noise-like share.

Consider the pixel value $H^{x,y}$ as the sum of RGB color values of (x, y) pixels. Therefore it can be represented as

$$H^{x,y} = \sum_{\emptyset \in \{R,G,B\}} P_{\emptyset}^{x,y} \quad (1)$$

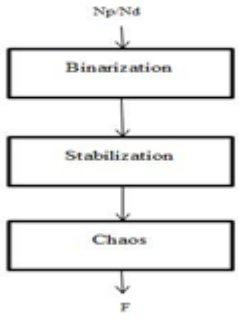

Fig 2. Feature Extraction Process.

Feature extraction process works in three phases: Binarization, Stabilization, Chaos [5]

Binarization

Binarization process extracts binary feature matrix from the natural images N. The feature value of each pixel can be calculated by using threshold function. The median M of the pixels in same block is calculated and set as threshold. Then each feature value of pixel is compared with the threshold. If the feature value is greater than or equal to M then the feature value is set to 1 otherwise it is set to 0.

$$f(x,y) = \begin{cases} 0, & H^{x,y} < M \\ 1, & H^{x,y} \geq M \end{cases} \quad (2)$$

Stabilization

The binary feature matrix obtained from binarization process may contain unequal number of 0s and 1s (0= black pixel, 1=white pixel). Stabilization is used to equalize the occurrence of black and white pixels in the matrix.

occurrence of unbalanced black Pixel is Q_s is determined as

$$Q_s \in [\sum_{x=1,y=1}^{x=b,y=b} f(x,y)] - \frac{b^2}{2} \quad (3)$$

Chaos

In the natural images the pixels with similar values may gather in the same region. This may cause the feature image as well as share to reveal some texture during encryption phase. The chaos process discards this appearing texture. It disorders the original matrix by adding noise to it.

The candidate pixels Q_c after adding noise P_{noise} is given by

$$Q_c = \frac{b^2}{2} \times P_{noise} \quad (4)$$

After feature extraction the bit-plane of the share image is generated by XORing the bit plane of secret image and n-1 feature matrix.

Image Preparations and Pixel Swapping Processes

These processes are applied before processing printed images and also after processing the feature matrices. In this the printed natural image must be first captured by some device such as digital scanners to convert them into digital format [5]. It is then followed by cropping and resizing where the image is resized to the size equivalent to natural share.

3) Encryption Technique

This scheme encrypts the color secret image by using n-1 natural images. The feature image generated from the feature extraction process is XORed with the secret image to produce a noise-like share.

Feature Extraction Algorithm

Input: N, b, P_{noise}

Output: F

Algorithm Feature Extraction ()
Step 1: Divide N into b x b blocks
Step 2: For every block repeat step 3-11
Step 3: For x= 1 to b, and y=1 to b calculates $H^{x,y}$ by eq. (1)
Step 4: Calculate M
Step 5: For x= 1 to b, and y=1 calculate $f(x,y)$ by eq.(2)
Step 6: Determine Q_s by eq.(3)
Step 7: Randomly pick Q_* pixels where $f(x,y)$= 1 and $H^{x,y}$= M. Let $f(x,y) = 0$
Step 8: Calculate Q_c by eq.(4)
Step 9: Randomly select Q_c where $f(x,y) = 1$
Step 10: Randomly select Q_c where $f(x,y) = 0$
Step 11: Swap the value of $f(x,y)$in step 9 and 10
Step 12: Output F

Encryption Algorithm

Input: SEI, Np, Nd, b, P_{noise}, t, ρ
Output: S'
Algorithm NVSSEncryption()
Step 1: Initialize random number generator G by the seed ρ
Step 2: n=Np + Dp + 1
Step 3: Initialize all feature images FI=0
Step 4: Repeat step 5 and 6 for i=0 to 7 for ϕ={R,G,B}
Step 5: Extract binary feature matrix from a N by calling algorithm Feature Extraction
Step 6: Add the extracted matrix to corresponding bit and color planes of F.
Step 7: If printed image np =0, goto step 12
Step 8: Repeat step 9-11 t times
Step 9: Randomly select one pair of pixels in a feature image
i.e. (x1, y1), x1 ϵ [1,w], y1 ϵ [1,h]
Step 10: Randomly select one pair of pixels in a feature image
i.e. (x2, y2), x2 ϵ [1,w], y2 ϵ [1,h]
Step 11: Swap the values of two pixels
$P_{\omega}^{x1,y1}$ and $P_{\omega}^{x2,y2}$
Step 12: Stack input image S and all feature images by applying the XOR operation in each color plane
S' ← ESI ⊕ FI1 ⊕ FI2 ….⊕ FIn
Step 13: Output S'

4) Applying Cover Image

This technique combines the cover images and secret image share S' for security purpose. It does not give any clue that some secret image or secret data is embedded with it. Hence, the security is increased. After embedding the secret share with cover image the generated image is transmitted over network to the receiver.

B. Receiver Side Architecture

The proposed receiver side consists of modules such as Extracting share from cover image, Natural image processing module and Decryption module.

When the receiver receives the secret image share embedded behind cover image, it first extracts the secret share from the cover image. To decrypt the share it performs same feature extraction process on n-1 natural images as performed by the sender.

After feature extraction the bit-plane of the secret image is generated by XORing the bit plane of noise share and n-1 feature matrix. In this way the receiver reveals the secret image. Then the encrypted data hidden behind the secret image is retrieved. This data is then deciphered using cryptographic technique to generate the original data.

In this way, receiver can receive the secret message as well as secret image securely.

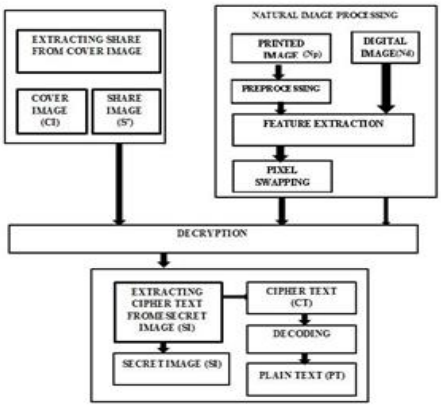

Fig 3. Receiver Side block diagrams.

Decryption Algorithm

Input: S', Np, Nd, b, P_{noise}, t, ρ
Output: ESI
Algorithm NVSSDecryption()
Step 1: Initialize random number generator G by the seed ρ
Step 2: n=Np + Dp + 1
Step 3: Initialize all feature images FI=0
Step 4: Repeat step 5 and 6 for i=0 to 7 for ϕ={R,G,B}
Step 5: Extract binary feature matrix from N by calling algorithm Feature Extraction
Step 6: Add the extracted matrix to corresponding bit and color planes of F.
Step 7: If printed image np =0, goto step 12
Step 8: Repeat step 9-11 t times
Step 9: Randomly select one pair of pixels in a feature image
i.e. (x1, y1), x1 ϵ [1,w], y1 ϵ [1,h]
Step 10: Randomly select one pair of pixels in a feature image
i.e. (x2, y2), x2 ϵ [1,w], y2 ϵ [1,h]
Step 11: Swap the values of two pixels
$P_{\omega}^{x1,y1}$ And $P_{\omega}^{x2,y2}$
Step 12: Stack input image share S' and all feature images by applying the XOR operation in each color plane
ESI ← S' ⊕ FI1 ⊕ FI2 ….⊕ FIn
Step 13: Output ESI
The output of NVSSDecryption() is secret image embedded with secret data i.e. ESI. Then ESI is decomposed into Secret Image (SI) and Cipher Text (CT). The CT is converted into plain text (PT) by using cryptography algorithm.
This can be mathematically represented as Step 1: SI + CT ← ESI
Step 2: PT← D (CT, K)
Hence we get Secret Image (SI) and Plain Text (PT) as final output.

IV. EXPECTED RESULTS

In Fig. 4, the plain text (PT) is taken as input which is converted to cipher text (CT) which is in unreadable form. This cipher text is hidden behind the secret image which is shown in Fig. 5.

After embedding cipher text it produces embedded secret image (ESI) which looks similar to SI. For feature extraction process, three natural images are taken in Fig. 6. These images are converted into feature image by feature extraction process.

The image taken for feature extraction can be in any format (eg. .bmp, .jpeg, .jpg etc). Fig. 7 (a) shows share S'

Fig. 6 shows three natural images. Fig.7 (b), (c), (d), (e) shows that performing XOR on any set of feature image with share does not reveal the secret. The secret is revealed only when all the feature images are XORed with the share S'.

This is the reason that this scheme is more secure. Fig. 8 shows the extraction of cipher text from secret image. Fig. 9 shows conversion of cipher text to original plain text. Hence the output at receiver side is original plain text and secret image.

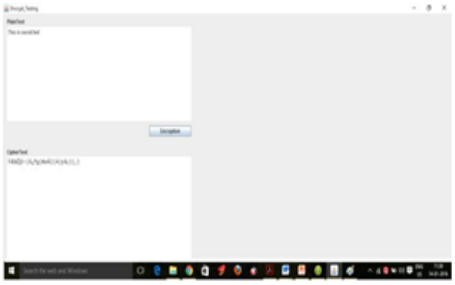

Fig 4. Encryption of Plain Text.

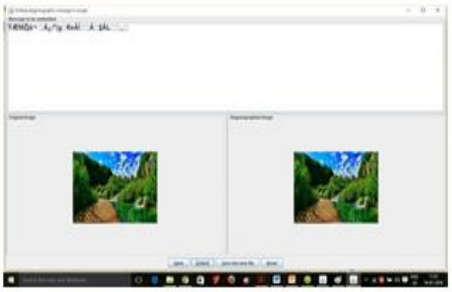

Fig 5. Embedding cipher text in secret image.

Fig 6. Natural Images used in feature extraction.

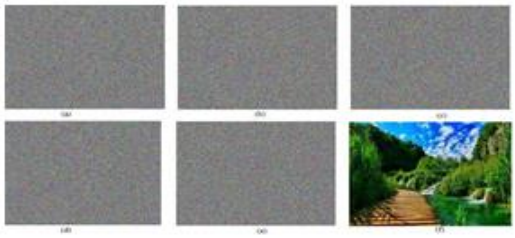

Fig 7. (a) share S', (b) S ⊕ FI1, (c) S' ⊕ FI1 ⊕FI2, (d) S' ⊕ FI1 ⊕ FI3, (e) S' ⊕ FI2 ⊕ FI3, (f) Recovered image of ESI (S'⊕FI1⊕ FI2 ⊕FI3).

Fig. 8:Extracting cipher text from secret image.

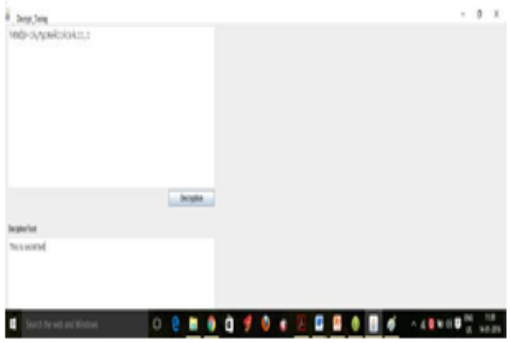

Fig 9. Decryption of Cipher text to plain text.

V. CONCLUSION

NVSS scheme can be applied to share image using different image media. This scheme can be useful in sharing a color secret image using natural image. Using this approach the risk associated with transmission as well as share management problems is solved. Steganography is included to securely transfer data by first encrypting it and then hiding it behind the image. The secret image is then encrypted and embedded in cover image. Hence this scheme is used to secure both data as well as secret image by applying data hiding along with NVSS scheme. This scheme also reduces the problem of pixel expansion. This scheme can share black and white, gray-level or color images secretly.

REFERENCES

[1] Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in Cryptology—EUROCRYPT'94. Springer Berlin/Heidelberg, 1995.

[2] Zhou, Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." Image Processing, IEEE Transactions on 15.8 (2006): 2441-2453.

[3] Ulutas, Mustafa. "Meaningful share generation for increased number of secrets in visual secret-sharing scheme." Mathematical Problems in Engineering 2010 (2010).

[4] Liu, Xiao-Yi, Ming-Song Chen, and Ya-Li Zhang. "A new color visual cryptography scheme with perfect contrast." Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on. IEEE, 2013.

[5] Lee, Kai-Hui, and Pei-Ling Chiu. "Digital image sharing by diverse image media." Information Forensics and Security, IEEE Transactions on 9.1 (2014): 88-98.

[6] Askari, Nazanin, Cecilia Moloney, and Howard M. Heys. "A novel visual secret sharing scheme without image size expansion." Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on. IEEE, 2012.

[7] Lee, Kai-Hui, and Pei-Ling Chiu. "Image size invariant visual cryptography for general access structures subject to display quality constraints." Image Processing, IEEE Transactions on 22.10 (2013): 3830-3841.

[8] Sasaki, Motoharu, and Yoshihiro Watanabe. "Formulation of visual secret sharing schemes encrypting multiple images." Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on. IEEE, 2014.

[9] Lin, T. L., Horng, S. J., Lee, K. H., Chiu, P. L., Kao, T. W., Chen, Y. H., & Chen, R. J. "A novel visual secret sharing scheme for multiple secrets without pixel expansion." Expert systems with applications 37.12 (2010): 7858-7869.

[10] Ulichney, Robert. "The void-and-cluster method for dither array generation."SPIE MILESTONE SERIES MS 154 (1999): 183-194.