International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secured Digital Image Sharing by using NVSS

Pramod Shimgekar[1], Kishor Wane[2]

[1]Department of ENTC, Dhole Patil College of Engineering, Savitribai Phule Pune University, Pune, India

[2]Professor, Department of ENTC, Dhole Patil College of Engineering, Savitribai Phule Pune University, Pune, India

Abstract: ***Conventional visual secret sharing schemes hide secret images in the form of shares that are printed on transparencies and stored in a digital form. The generated shares appear as noise-like pixels; but it will stimulate suspicion and increase the interception risk during transmission of the generated shares. Hence, visual secret sharing schemes experience from a transmission risk problem for both the secret data image and for the participants who are involved in the sharing process. To tackle this problem, the proposed natural-image-based visual secret sharing scheme (NVSS scheme) shares secret images via various transporter media to protect the secret data image and the participants during the transmission phase. A very significant role is played by Encryption and decryption algorithms to transmit digital images securely from source to destination. Number of encryption and decryption algorithms is available in order to encrypt the task. The proposed analysis over the different sets of the image by using the three different Encryption and Decryption algorithms is performed. The comparison is made over the analysis made by using the different parameters such as PSNR value, Bi-Linear PSNR value, MSE (Mean Square Error) value, Elapsed time required or Encryption and Decryption process. Implementation and analysis of different selective image encryption and decryption technique is made in this paper by using Matlab.***

Keywords: visual cryptography, visual secret sharing, natural image based visual secret sharing.

1. Introduction

Visual Cryptography (VC) is a technique that divides a secret data image into n shares, with each participant holding one or more shares. Anybody who holds fewer than n shares cannot reveal any information about the final secret data image. To reveal the secret image the participant has to stack the generated n shares and after regeneration of the image it can be recognized directly by the human eyes. The Cryptography is a technique of converting the original data into a scribbled encrypted format called the cipher text. The technique to encode the secret data which will protect it while transmission can be achieved by making use of cryptography, it makes use of hash function that uses some mathematical function to achieve the technique to encode the secret data. This technique is basically used in military, ecommerce and to transmit confidential data. Secret data images can be of various types: images, photographs, handwritten documents, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme.

Sharing secret images has become an important issue today. The generated shares consist of many arbitrary and meaningless pixels which satisfies the security requirement for protecting secret contents to be transmitted, but they will experience two drawbacks: first, high transmission risk is present because of generated noise-like shares will cause attackers doubt and the shares may be detected. Thus, the risk to both the participants and the shares increases, in turn increasing the possibility of transmission failure. Second, the meaningless shares are not user friendly.

The encryption and the decryption process can be of different types, and thus can improve the quality of sharing an image securely. The proposed paper has taken the three algorithms for comparing the results and making analysis about the best suited encryption and decryption algorithm among the three. The different encryption and decryption algorithms include the AES algorithm, the CHAOTIC based algorithm and the basic encryption and decryption algorithm which works on the image to encrypt it with high security in order to share it at various levels secretly. AES algorithm is the one which make use of a single key used for both encryption and decryption. Traditional symmetric ciphers such as Advanced Encryption Standards (AES) are designed with good confusion and diffusion properties. The chaotic based encryption and decryption algorithm works on the alterations of the pixel values. This algorithm produces a cipher of the test image that has good diffusion and confusion properties. The third algorithm used is referred as the basic algorithm for encryption and decryption; it works by performing the quantification by a certain factor. The result of the analysis has been distributed about the PSNR values, Bi-Linear PSNR value, MSE (Mean Square Error) value, Elapsed time required or Encryption and Decryption process.

2. Proposed Theory

The paper propose a visual secret sharing (VSS) scheme, called the natural image–based VSS scheme (NVSS scheme), to reduce the intercepted risk during the transmission phase. In the proposed scheme, various media for sharing digital data images is used. The various carrier media in the scheme includes printed images, digital images, hand-painted pictures, and images taken from a camera etc. Applying a diversity of media for sharing the secret image increases the degree of difficulty of intercepting the shares. The proposed NVSS scheme can share one digital secret image over n - 1 random selected natural images (natural shares) and one noise-like share. Here instead of altering the contents of the natural shares it just extracts the features of the natural shares. These unaltered natural shares are totally harmless thus greatly reducing the interception probability of these shares. The generated share which is noise-like can be hidden by using data hiding techniques to increase the security level and making it more secure and easy to send during the transmission phase. The NVSS scheme uses diverse media as a carrier; hence the dealer can choose an

image that is not easily suspected as the content of the media to reduce the transmission risk. The generated digital shares can be stored in a participant's digital devices (e.g., digital cameras, computers, laptops, tablets, smart phones) to reduce the risk of being suspected. The printed media (e.g., hand-painted pictures) can be sent via postal or direct mail marketing services or even my e-mail. In such a way, to increase the security for the shared images the transmission channels are also diverse, further reducing the transmission risk. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of both participants and shares.

3. Literature survey

According to chengguo, chin-chenchang, chuanqin [1] by using the multi-threshold access sharing of secret image in groups can be achieved. Using this approach multiple secret images can be shared with different group of participants and each image is associated with different access structure. To propose a multi-threshold secret image sharing scheme author has used Hsu et al's multi secret sharing scheme which is based on MSP (Monotone Span Program). In this scheme corresponding access structure are pre-defined. According to these access structures shadow data can be achieved from multiple secret images by using Hsu et al's method by making use of Least Significant Bit (LSB) replacement can be used to embed the shadow data into the cover images. By collecting a corresponding subset of shadow images each lossless secret image can be reconstructed. The proposed scheme first generates the shadow data. These shadow data is then embedded in the cover image. The integrity of the shadow image is verified in order to avoid the false shadow image transfer to participant during the recovery of the secret image. Then the secret image is retrieved. Thus this scheme is feasible and can achieve high visual quality of shadow image and high embedding capacity.

Kai-hui lee and pei-ling chiu [2] has proposed an extended visual cryptography algorithm for general access structure. The previous approaches suffer from pixel expansion problem. The extended visual cryptography add meaningful cover images in each generated share. The proposed scheme can be used for binary secret images present in non-computer environment. The proposed approach consists of two phases. The first phase is based on given access structure in which meaningless shares are generated using an optimization technique. In the second phase stamping algorithm is used to directly add the cover image in each generated share. Hence by using the proposed approach the pixel expansion problem of EVCS for general access structure is achieved. The display quality of the recovered image is also good.

Tzung-Her Chen and Kai-Hsiang Tsao [3] proposed that in 1987 kafri and keren stated the visual secret sharing technique which was based on random grid. In this scheme pixels of secret image and natural image are divided into two grades grade1 and grade2 depending on which pixel is move on which grade. And at the receiving end grade1 and grade2 is combined, then depending on which pixel belong to which grade move the pixel in grade1 and grade2.In this paper they propose that the pixel expansion is not introduced in random grid visual secret sharing the first random grid G1 is achieved by selecting the white or black color. Then it is provided to a certain private pixel to resolve the grid pixel of G1 and grid pixel of G2. G1 and G2 stacked results are always fully black although the private is black and white or black with ½ probabilities although the private is white. In this way the private is recognizable through stacked random grid.

Pei-Ling Chiu and Kai-Hui Lee [4] has proposed that a threshold visual cryptography scheme is considered of more than one secret data image and n-number of natural images. Only binary image is considered in Threshold visual cryptography scheme. In order to increase the computation cost and degrade the performance, In the proposed paper, an optimization technique is in order to encipher unseen binary images. Blackness is recognized as a resourceful metric in the display quality measurement ofan output image. The problem is first solved as a mathematical optimization in order to exploit the contrast of the output image. To solve this problem they establish a encouraged annealing based algorithm.

InkooKang,Gonzalo.R.Arce and H.K.Lee [5] proposed that the meaningful shares are generated due to encoding of secret image in generated shares by using a visual cryptography encryption method. Color visual cryptography is depended on two principles, one is error diffusion and another is visual information pixel synchronization. Error diffusion is for image halftone generation and synchronization which improves the contrast of shares. The error diffusion in general generates the shares which are pleasant to the human eyes, by synchronizing the visual information pixels beyond the color channels visual contrast of shares can be made better. The paper states the encryption method which improves the visual quality by constructing color extended visual cryptography with VIP synchronization and error diffusion. the original VIP values and the shares of visually high quality is present in before encryption VIP synchronization and after encryption VIP synchronization also.

Z. Zhou, G. R. Arce, and G. D. Crescenzo [6] proposed a framework of common halftone visual cryptography (HVS), where a personal binary image is hidden into halftone share. Blue noise halftone technique is applied in order to generate the halftone shares. These generated halftones are used to transfer the important visible data to the participant like photography, scenery, paintings, and images. The visible character obtained through this current plan is better in comparison made to the extended visual cryptography. In the reviewed paper the technique used to obtain visual cryptography through halftone, is halftone visual cryptography technique. In this method the void and cluster algorithm is used to encrypt a binary personal image into 'n' number of halftone shares which includes the significant visual information. The proposed method generates the visually attractive halftone shares which carry important data better Visual quality is obtained than other available visual cryptography method.

Rui Liu et al [10] proposed a SBLP and chaotic map to encrypt color image with the key. Firstly the position of image pixels is shuffled by using Logistic chaotic sequence and in order to rearrange the position of the image pixels another Logistic map is used. In this paper the author has made security analysis and experimental results such as, Histogram analysis Correlation analysis, UACI and NPCR as well as key sensitivity analysis are also performed.

HuibinLu et al [11] has proposed an algorithm based on Chen and Lorenz systems to encrypt color images implemented in MATLAB 7.0 with the key space. In this algorithm, firstly the information of image is integrated into the Lorenz map, and then it is mixed by using the Lorenz map into the Chen map. Correlation analysis of two adjacent pixels, Entropy analysis and Histogram analysis, NPCR, UACI as well as key space and sensitivity analysis is made by the author in this paper to prove the security of the algorithm. The infeasibility of Brute-Force attacks and Resistance attack has also been verified by the author.

4. Methodology

Initially Secret Image and Natural Images has been Chosen. Natural Images would be Painted and Digital Images. The image preparation processes are used for preprocessing printed images and for post-processing the feature matrices that are extracted from the printed images.

The flow of Image Preparation process is: The contents of the printed images can be acquired by popular electronic devices, such as digital scanners and digital cameras. The next step is to crop the extra images. Finally, the images are resized so they have the same dimensions as the natural shares. In order to be used in an encryption module and decryption module without any fault, then the pixel swapping is performed to randomize the spatial correlation of pixels in a printed image. The generated shares are encrypted in the encryption process in order to be transmitted. These shares after receiving are decrypted by the decryption module and the secret shared image is obtained.

The above procedure is repeated for all the three algorithms which are used for analysis. The results of all the algorithms are compared and the graph is plotted with the related data. The certain database is being prepared for the comparison. The database consists of the sets of different image over which the analysis s done.

The sets includes the images from the natural scenes, hand painted pictures, images from different cameras, different wallpapers etc. database is prepared by using the different images or a set of images. Each set includes one base image and one secret image. About 50 sets of different image have been prepared for the analysis purpose. The database has worked over the three different algorithms.

1) AES Algorithm:

***Encryption phase*:**
The steps used to achieve the proposed security technique are as follows:
Step1: Initially, the position number of each byte in the text file is added to its corresponding ASCII value. The modified ASCII value is then stored in the file.
Step2: In the second step, every bit in the input file is manipulated according to the length of the password provided by the user.
Step3: In the next step, after converting each byte of the input file into its binary equivalent, blocks of data are taken and advanced bit randomization technique is applied.
Step4: In the fourth step, the bits in the file are reversed using Bit reversal technique. Thus the output of this step will be the encrypted cipher text.
Step5: In this step, the encrypted file is embedded into the image by modifying the LSB of the image with respect to the bytes of the encrypted file.
Step6: Finally, a pattern is set for the image within which the encrypted file has been embedded.

Decryption phase:
In the decryption phase, the hidden information can be extracted when all *n* shares are received; the decryption end extracts *n* -1 feature images from all natural shares and then executes the XOR operation with encrypted image to obtain the recovered image. The first step in decryption phase to check whether the provided key is same as it was provided during encryption process. If the key is not matched then the process will not execute further and the image cannot be extracted. If the correct key is provided then the reverse steps of encryption process is applied. MSA is applied then the it manipulation is done first then XOR operation is performed to the 8-bit binary data obtained from the ASCII values here the XOR operation is in the reverse form from grey code to binary. Randomization bit manipulation is done to convert binary to decimal and thus the altered ASCII values are obtained.
PSNR value is calculated.
Bi-Linear PSNR value is calculated.

2) CHAOTIC Algorithm:

Encryption phase:
Step1: The 16 bit key is used for the Encryption and decryption.
Step2: The key should be less than or equal to 16-bit. Then the second step is of bit manipulation. Bit manipulation is done in order to convert the letters to the corresponding ASCII values. The generated ASCII values are converted to the 8-bit binary data.
Step3: Key is generated by using the indices of image which is referred as Fkey.
Step4: Encrypted image is created by using the XOR operation. The XOR operation is performed over image and which is generated known as Fkey.

Decryption phase:
The reverse process is performed for revealing the secret image.
PSNR value is calculated.

Bi-Linear PSNR value is calculated.

3) Basic Algorithm:

Encryption phase:
Step1: The cover image is selected.
Step2: Secret image is selected.
Step3: The encryption key is selected which is between 0-255.
Step4: The encryption key entered is checked whether it is less than 255.
Step5: The cover image values are rounded off to its nearest value.
Step6: Decryption key is entered and compared with the encryption key entered
Step7: If the key entered is equal to the encryption key entered than the decryption phase is executed and the secret image is revealed.

Decryption phase:
The reverse process is performed for revealing the secret image.
PSNR value is calculated.
Bi-Linear PSNR value is calculated.

5. Experimental Result

The experiment is performed over the database of more than 50 images. The result shows us the relative comparison between the PSNR values, The Bi-Linear PSNR values, the timing analysis between the encryption and the decryption of the image, the MSE (Mean Square Error) calculated. On the basis of these values the analysis about the encryption and the decryption algorithms best suited for the transmission of the secret image or data securely within the participants can be made.

In the experimental results shown below is performed over a single set of image. Which include one secret image and one base image.

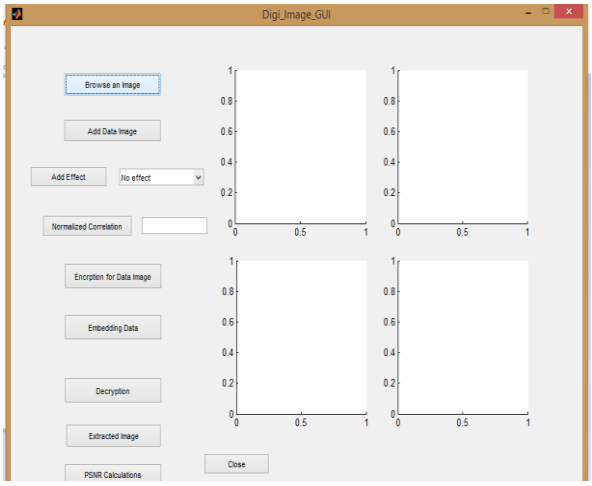

Figure 1: Basic GUI

Figure 2 (a): Base image **Figure 2 (b):** secret image

1) PSNR value is calculated and comparison is shown in fig.3 (a).

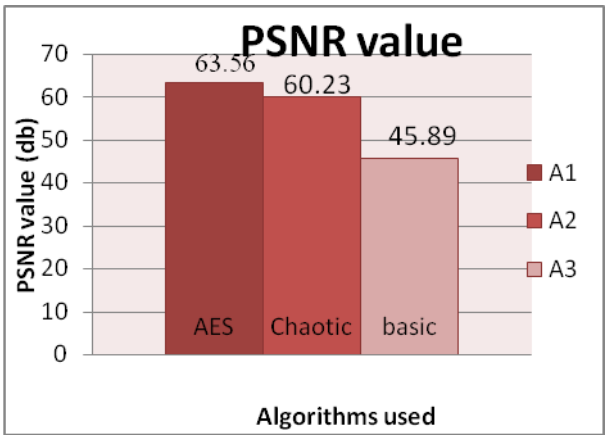

Figure 3 (a):

2) Bi-Linear PSNR value is calculated and comparison is shown in fig.3 (b).

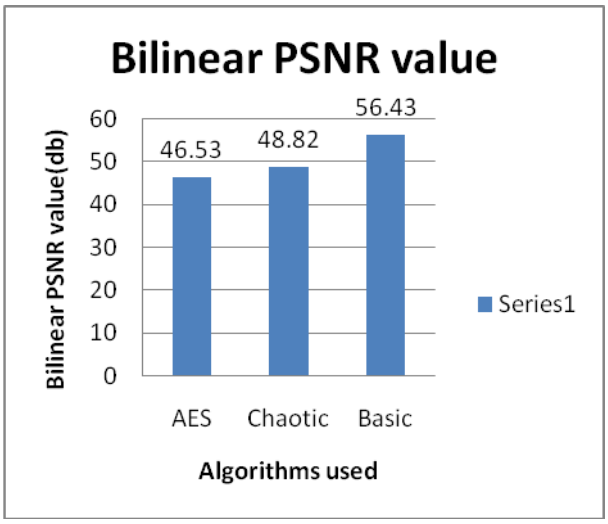

Figure 3 (b):

3) Mean Square value is calculated and comparison is shown in fig.3 (c).

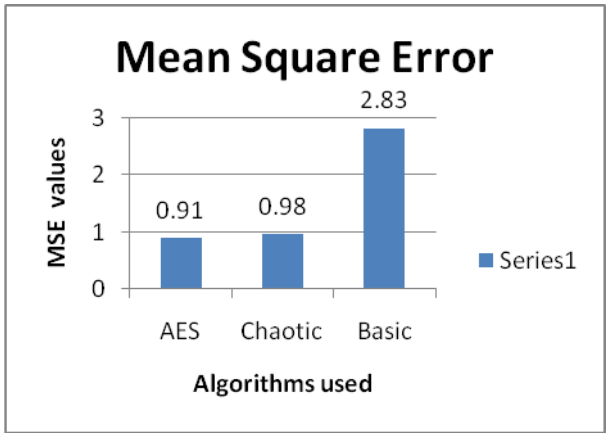

Figure 3 (c)

4) The elapsed time is calculated and the comparison is shown in fig.3 (d).

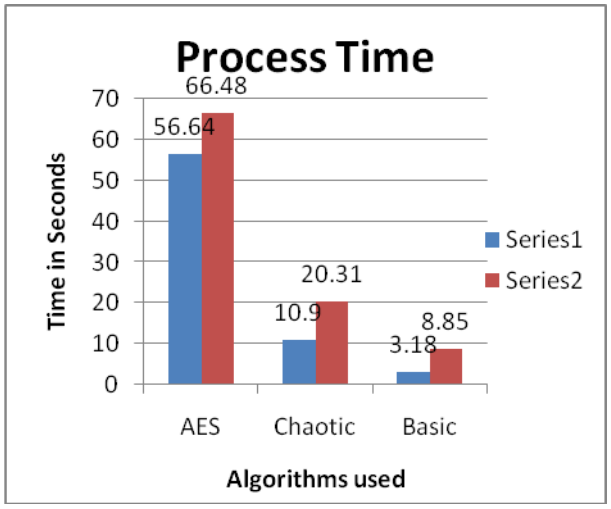

Figure 3 (d)

5. Conclusion

The proposed natural image based visual secret sharing scheme can share a digital image using a diverse media of images. The media includes the randomly chosen images which are unaltered in the encryption phase. Therefore they are totally innocuous. The comparison results shows that the AES algorithm used for Encryption and Decryption purpose is more secure and the error between the secret image transmitted and received is less than the Chaotic and the Basic Encryption and Decryption algorithm used. The proposed analysis can effectively reduce the transmission risk and provide the high level of user friendliness for both, the shares and the participants.

References

[1] C. Guo, C. C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," Pattern Recognit. Lett., vol. 33, no. 12, pp. 1594–1600, Sep. 2012.
[2] 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.
[3] Tzung-Her Chen and Kai-Hsiang Tsao," User-Friendly Random-Grid-Based Visual Secret Sharing," ieee transactions on circuits and systems for video technology, vol. 21, no. 11, november 2011.
[4] Pei-Ling Chiu and Kai-HuiLee,"A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes,"ieee transactions on information forensics and security, vol. 6, no. 3, september 2011.
[5] 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.
[6] Z. Zhou, G. R. Arce, and G. D. Crescenzo"Halftone visual cryptog- raphy," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
[7] A. Nissar and A. H. Mir, ―Classification of steganalysis techniques: A study,‖ *Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, Dec. 2010.
[8] 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.
[9] 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.
[10] Rui Liu, Xiaoping Tian, "New Algorithm For Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation", Journal of Theoretical and Applied Information Technology, Vol.43, No.1, 2012, pp. 89-93.
[11] Huibin Lu, Xia Xiao," A Novel Color Image Encryption Algorithm Based on Chaotic Maps",Advances in information Sciences and Service Sciences(AISS), Volume3, Number11.

Author Profile

Pramod shimgekar received a bachelor's degree in Electronics and Telecommunication from Sipna shikshan Prasarak Mandal's College of Engineering and Technology, Sant Gadge Baba Amravati University, Amravati in 2012.He is now pursuing his master's degree in VLSI and Embedded Systems from Dhole Patil College of Engineering and Technology, Savitribai Phule Pune University, Pune, India.