Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

# IMPLEMENTATION OF VISUAL CRYPTOGRAPHY USING NVSS SCHEME IN A ETC SYSTEM

Prof. Alok Chauhan[1], Miss.Swati B. Patil[2]
[1]Asstt. Professor, Department of Information Technology
R.G.C.O.E.R, Nagpur,Nagpur University, Maharashtra, India
[2]M.Tech Student,PG Department of Computer Science and Engineering
R.G.C.O.E.R, Nagpur,Nagpur University, Maharashtra, India

**ABSTRACT-**Secret images in Conventional visual secret sharing are hidden in shares that are either encoded and stored in digital form or printed on transparencies. The shares can be meaningful images or noisy like image, which may arouse suspicion and may be intercepted. Thus VSS Schemes are risky for the participants who are involved and even for the secret. In order to counter the above problem natural image based VSS Scheme is used that shares the secret image through various communication media to safeguard the participants and the secrets. In (n, n) NVSS scheme, one Secret image is shared over n-1 randomly selected natural images (natural shares) and one noise like image .The secret image and natural shares (in print form) generates the noise like image. The Natural Shares are commonly found and diversity of their selection drastically reduces the suspicion. The system may be made more efficient by introducing the concept of Encryption then Compression(ETC) unlikely the concept of compression then Encryption(CTE).After generating the noise like image by encryption ,it is hidden the compressed and transmitted. The process is reversed at the receiver end. Thus combination of (n, n) NVSS Scheme and ETC gives excellent solution for transmission risk problem.

**Keywords-**Visual secret sharing scheme, natural images, transmission risk, Encryption- Then-Compression system.

## I. INTRODUCTION

Image processing is any form of signal processing where the input can be an image and the output may be either an image or a set of parameters related to the image. With the invention of the Internet, more and more digital data can be accessed via the network. Internet users can transmit and store images with less secured channels. To secure the information one possible technique is cryptography where information is encrypted using key and same key is used to decrypt the information. Here computation complexity of decryption algorithm increases the information security [1].

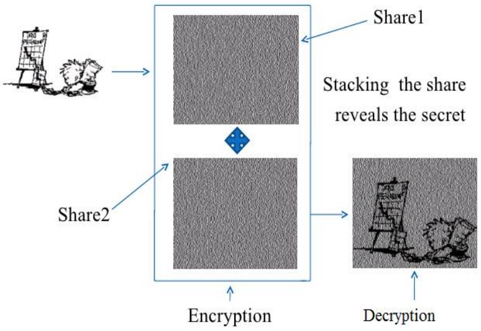

*FIG 1: OVERVIEW OF VISUAL CRYPTOGRAPHY*

Image processing is any form of signal processing where the input can be an image and the output may be either an image or a set of parameters related to the image. With the invention of the Internet, more and more digital data can be accessed via the network. Internet users can transmit and store images with less secured channels. To secure the information one possible technique is cryptography where information is encrypted using key and same key is used to decrypt the information. Here computation complexity of decryption algorithm increases the information security [1]. Visual Cryptography is a technique which provides information security and uses simple decryption algorithm unlike the computationally complex algorithms used in traditional cryptography schemes. This technique allows Visual information such as pictures, text, etc. to be encrypted in such a way that their decryption can be performed by the human visual system. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image.

With the advent of transmitting multimedia data over the internet, it has become important that the security of data be given much importance. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

VISUAL CRYPTOGRAPHY (VC) is a type of secret sharing scheme introduced by Naor and Shamir [2].Visual secret sharing allows us to share the image, but there is an interception risk problem during transmission phase.  A Natural visual secret sharing (NVSS) scheme uses various carriers' media for transmission so that there cannot be interception risk problem. This New NVSS scheme can share one secret image over n-1 arbitrarily natural images .These natural images can be printed images and digital images. The n-1 natural shares act as keys to encrypt/decrypt one secret image. So a process is known as (n,n)NVSS scheme. This process of encryption/decryption is implemented in an Encryption-then-compression/stenography (ETC) system, where the encrypted image is compressed or hidden in any natural image and sent to the receiver end.

## II. RELATED WORK

From the Carrier viewpoint VSS Scheme uses Transparency, Digital media, printed media for transmission. Previous research used only transparencies and digital media as carrier for a VSS scheme. A VSS Scheme using Transparency as a carrier media have noise like share or a meaningful appearance. The noise like share is not user friendly. So Researcher tried to improve the property of user friendliness in a VSS scheme. Another New Scheme EVSS reduced the display quality of the recovered image which did not reduce the interception risk during transmission.

Steganography is a technique used for hiding information and making the communication invisible which was adopted to hide the secret image[14][16] .So the hidden Information and its carrier can be protected. It was used to hide digital shares which can be concealed in cover image that are halftone gray image and true color image. Although this Stego images can still be detected Stegnalyst method [17].

A new Scheme called NVSS Scheme is developed where a secret image is shared via natural images. In this study we make an extension to the previous work where possibility of adopting the unaltered printed media as share was adopted. The share then is compressed after the encryption process which implements the ETC scheme. This compression work in a lossless image scenario.

## III. THE PROPOSED SCHEME

A new VSS Scheme called Natural image based VSS Scheme (NVSS Scheme) reduces the interception risk problem during transmission phase. The NVSS Scheme shares a digital secret image over n-1 arbitrary natural shares and one share. This uses a diverse image media as a carrier for sharing digital images. The carrier media contains digital images, printed images, hand-painted pictures; etc.Using diverse carrier image media increases the degree of difficulty of intercepting the shares. The contents of natural images/shares are not altered. These non altered natural shares are totally innocuous thus reduces the interception probability. The noise like share can be concealed by using various data hiding technique to increase the security the level during the transmission phase.

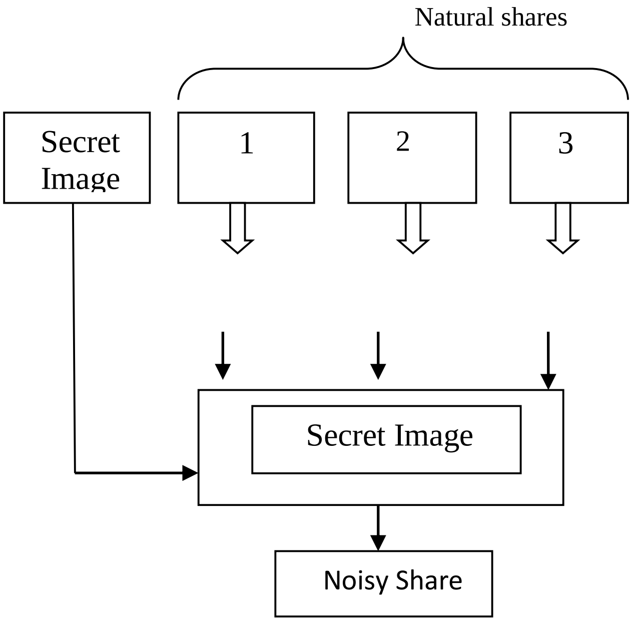

*Fig. 2. Process at the sender side*

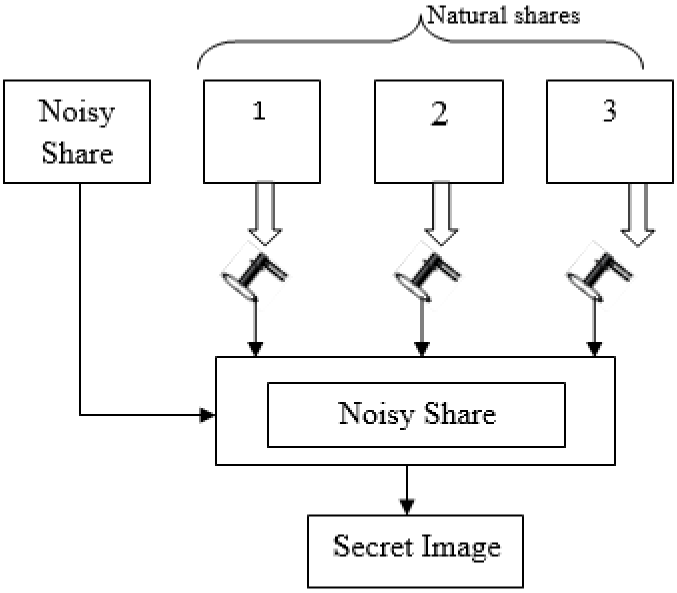

*Fig.3. Process at the receiver side*

The (n, n)-NVSS scheme takes arbitrary n - 1 natural shares and one generated share as carrier media to share one digital true color secret image that has 24-bit/pixel color depth. The objective is to reduce the transmission risk of shares by using diverse and innocuous media.

1. As the number of delivered shares increases, the transmission risks increases.
2. The transmission risk of shares with a meaningful cover image is less than that of noise-like shares.
3. The transmission risk decreases as the quality of the meaningful shares increases.
4. The natural images without artificially altered or modified contents have the lowest transmission risk.

Natural shares

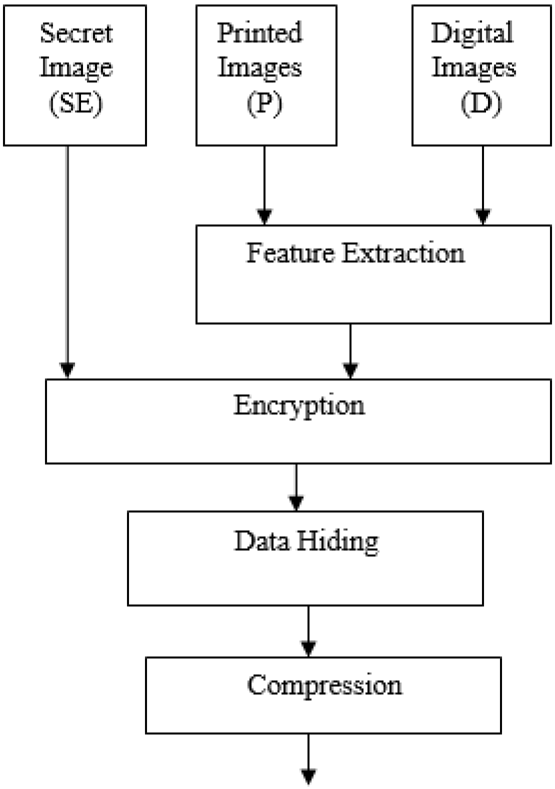

*Fig.4.a. Encryption Process*

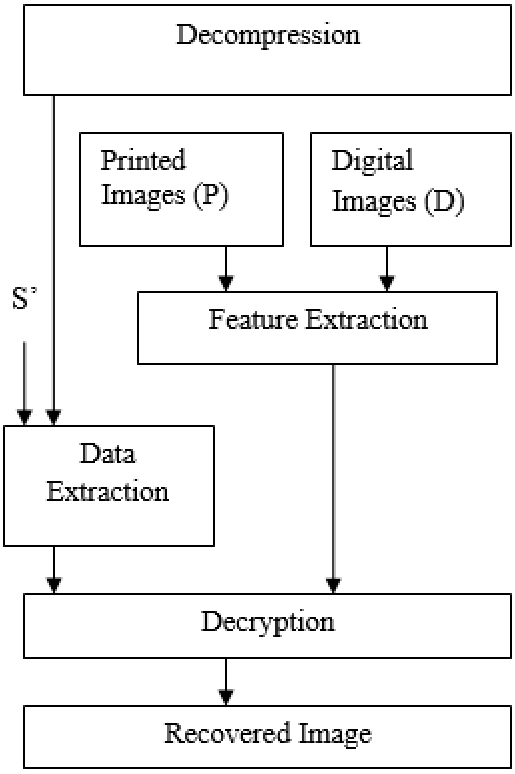

*Fig.4.b. Decryption Process*

## IV. THE FEATURE EXTRACTION

The feature extraction module consists of three processes—binarization, stabilization, and chaos processes. First, a binary feature matrix is extracted from natural image N via the binarization process. The stabilization balances the occurrence frequency of values 1 and 0 in the matrix. Finally, the chaos process scatters the clustered feature values in the matrix.

In binarization process, a set threshold is determined by a simple threshold function F to determine a binary feature value.Median M is calculated to obtain approximate appearance for binary values 0 and1.Median M is the threshold value.

Therefore

$$F(H^{x,y}) = \begin{cases} 1 & H^{x,y} \geq M \\ 0 & Otherwise \end{cases} \qquad \text{Eq.(1)}$$

In the stabilization process the number of black and white pixels are balanced in each block the number of unbalanced pixels $Q_s$ is calculated by using the formula

$$Q_s = \begin{pmatrix} \Sigma \forall x 1 \leq x \leq x_b f^{x,y} \\ \forall y 1 \leq y \leq y_b \end{pmatrix} - \frac{b^2}{2} \qquad \text{Eq. (2)}$$

Depending upon the value of Qs $f\ x,y=1$ is randomly selected and the values of these pixels is set to 0.

The third process of chaos is used to eliminate the texture which appears on the extracted feature image and the generated share. The original feature matrix is disordered by adding noise $Q_c$ number of black feature pixels $f\,x,y=0$ are altered to $f\,x,y=1$ and vice versa.$Q_c$ is calculated by the given formula

$$Q_c = \frac{b^2}{2} * \mathbf{P}_{\mathbf{noise}} \qquad \text{Eq. (3)}$$

$P_{noise}$ is the salt and paper noise whose value ranges from 0 to1 here $P_{noise}$ =0.5

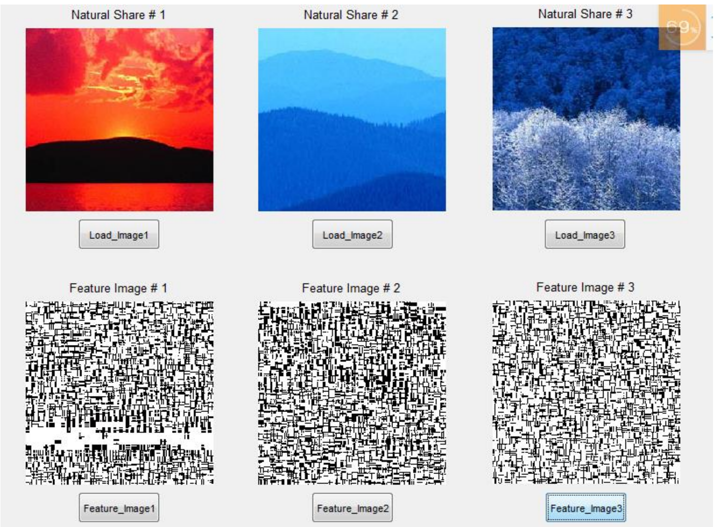

*Fig5. Graphical user interface of Feature extraction taking three natural shares at the sender side*

## V. RESULTS OF FEATURE EXTRACTION:

**Encryption/Decryption:**

The (n ,n)-NVSS schemes encrypts a true color secret image by n-1 natural shares and one noise share. Algorithm for encryption/ Decryption as follows.

Input S, $N_{1\ldots\ldots}$,Nnp+np,np,nd,b,Pnoise ,ρ,t
Output: $\overline{S}$

```
1.Initialize the random number generator G by the seed ρ
2. n $\leftarrow n_p + n_d+1$
3.$\forall$ $1<= \alpha < n$,$\forall$ $\varphi$ Є (R, G, B), $Fl\ \alpha,\varphi \leftarrow 0$
4.$\forall$ $1<= \alpha < n$, $\forall$ $\varphi$ Є (R, G, B), $\forall 0 <= i<=7$ repeat steps 5 to 6
5. Call procedure FE($N_a$,B,$P_{noise}$,F)
6.$\forall$(X,Y),x Є[1,h],$p^{x,y}_{\alpha,\varphi} \leftarrow p^{x,y}_{\alpha,\varphi}+f^{\,x,y} * 2^i$
7.If $n_p$=0 then goto step 12
8.$\forall$ $1<= \alpha <n_p$ repeat step 9-11 times
9. Randomly select $(x_1,y_1)$,$x_1$ Є[1,$w$],$y_1$ Є[1,h]
10. Randomly select $(x_2,y_2)$,$x_1$ Є[1,$w$],$y_2$ Є[1,h]
11$\forall\varphi$ Є(R,G,B),exchange value of $p^{x1,y1}_{\alpha,\varphi}$ and $p^{x2,y2}_{\alpha,\varphi}$
12$\forall\varphi$ Є(R,G,B), $\overline{S}_\varphi \leftarrow S_\varphi \oplus F1_{1,\varphi} \oplus F1_{n-1,\varphi}$
13.Output S
```

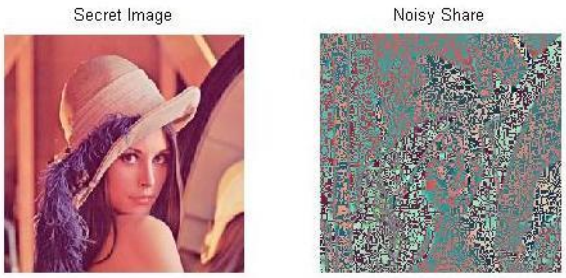

*Fig.6.a Encryption process*

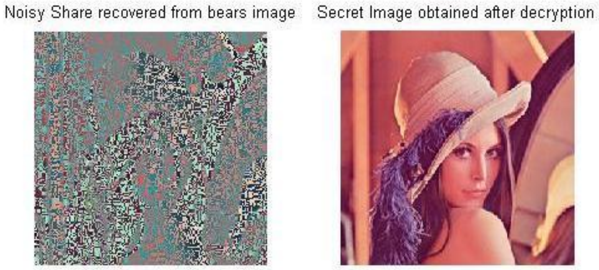
Noisy Share recovered from bears image
Secret Image obtained after decryption

*Fig.6.b.Decryption process*

## VI. SHARE HIDING/ COMPRESSION

After the encryption process, now the noise share is hidden and a new generated share is obtained by using the Share hiding algorithm. Now this generated share is compressed which clears the idea of this paper.i.e ETC scheme. First encrypting the image and then compressing it before sending on the transmission media. At the receiver side, in decryption phase reverse process is repeated. On receiving the compressed stego share, it is first decompressed; the hidden information is then extracted from the share. The share extraction algorithm is used for extracting a feature matrix. It is then decrypted with the help of Printed image and Digital Image and the original Image is recovered.

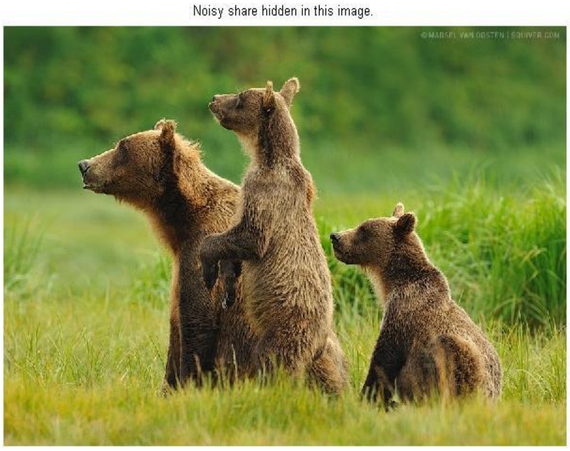

*Fig.7. Compression/hiding process*

## VII. CONCLUSION

The project focuses on image cryptography using (n,n) NVSS and Encryption–then-Compression system.

- Three processes namely Binarization, Stabilization, Choas is used for feature Extraction.

➢ A (n,n) NVSS encryption/decryption algorithm is used for encrypting the secret image and then decrypting the noisy share The noisy share developed at the sender side is hidden/compressed in another natural image which has no possibility of interception during transmission.

## 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 visualsecret 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 qualityand 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.

[14] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secretimage sharing scheme for true-color images with size constraint," *Inf.*
*Sci.*, vol. 179, no. 19, pp. 3247–3254, Sep. 2009.

[15] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image sharingscheme with reversible steganography based on cellular automata,"*J. Syst. Softw.*, vol. 85, no. 8, pp. 1852–1863, Aug. 2012.

[16] Kai-Hui Lee and Pei-Ling Chiu ,"Digital Image Sharing by Diverse Image Media" ieee transactions on information forensics and security, vol. 9, no. 1, january 2014.