

# Enhanced Data Security using Visual Data Hiding process

Shailesh Kumar<sup>#1</sup>, Er. Archana Singh<sup>#2</sup>

*# Department of Computer Science & Information Technology (SSET), SHIATS, Allahabad, India*

<sup>1</sup>shailesh.kumar159@gmail.com,<sup>2</sup>archana.singh@shiats.edu.in

**Abstract**—Image cryptography is an art of hiding information in images or transforming images to obtain to hide any visual information. The image cryptography is a traditional domain of information hiding and may be very old between various cryptographic techniques. In this modern age image cryptography is a mathematical model by which the information is manipulated in other human un-recognizable format. Basically that can be categorized in two basic classes first partial image encryption, and secondly the complete image encryption technique. In this paper the image cryptographic approach is explored and investigated for their authenticity. In addition of that a new cryptographic model is proposed and implemented. The basic idea is taken from a partial image encryption technique namely visual cryptography, and the idea is extended to find a complete image cryptographic scheme. Therefore, additional mathematical operators are utilized for achieving new cryptographic data model. Moreover it, the previous image cryptographic models are only suitable to encrypt image data. That is also extended to find a solution for text and image both kinds of data. The proposed cryptographic model is implemented using java technology. After implementation the performance of the proposed system is evaluated over different performance parameters i.e. computational complexity, space complexity and data validity. The calculated results demonstrate the acceptability of the proposed cryptographic model due to their less resource (memory and time) consumption, high data validity for image and text data both.

**Keywords**— Cryptography, visual cryptography, colour image, performance estimation

## I. INTRODUCTION

The art of preserving information by transforming it (encrypting it) into an unreadable format (for human eyes), called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to

everyone and a private key that only the recipient of messages uses.

In this study the image and text encryption scheme is proposed, basically the encryption algorithms are mathematical models that are manipulating the data to hide them. Therefore encryption algorithms are varying according to the data formats. Therefore for encryption and decryption of two data formats are a complex issue in this study. In addition of that successfully data recovery from modified message is also a complex task in presence of different data formats. Therefore a new innovative solution is tried to find in this proposed study work.

The proposed work is intended to provide an efficient and a complex cypher generation technique using the hybridization of different techniques. For successfully achieve the desired goal following tasks are included in the study.

1. Study of different image and visual cryptographic scheme: in this phase of study various image and visual cryptographic approaches are explored in order to find the appropriate solution.
2. Design and implementation of the new enhanced algorithm: a new image and text cryptographic technique is implemented in this module.
3. Performance analysis: in this phase the performance of the system is evaluated for finding the computational and storage complexity.















## II. BACK GROUND

This section provides the background of the cryptography and utilizing techniques.

### A. Visual Cryptography

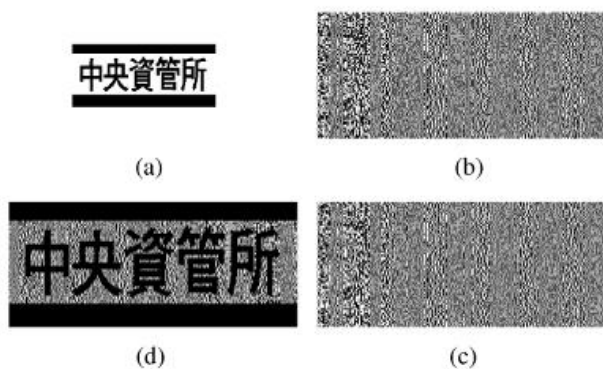
Because the output media of visual cryptography are transparencies, we treat the white pixels of black-and-white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into a 2×2 block in the two transparencies according to the rules in Fig. 1. When a pixel is white, the method chooses one of the two combinations for white pixels in Fig. 1 to form the content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations. Then, the

characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white.

Secret image	Share1	Share2	Stacked image
			
			
			
			

**Figure 1 : Sharing and Stacking Schemes**

Therefore, when stacking two transparencies, the blocks corresponding to black pixels in the secret image are full black, and those corresponding to white pixels are half-black-and-half-white, which can be seen as 50% gray pixels. As for information security, there are six possible patterns from which every block in a transparency can randomly choose, so the secret image cannot be identified from a single transparency. Take Fig. 2 for example. The secret image (a) with the words of Chinese letters is decomposed into two visual cryptography transparencies (b) and (c). When stacking the two transparencies, we can obtain the reconstructed image (d). Even though the contrast of the resulting image is degraded by 50%, human eyes can still identify the content of the secret image easily.



**Figure 2 : Visual Cryptography**

### III. PROPOSED WORK

Now in these days, most of the applications are becomes online. Online applications help to provide various services at door steps, due to this, demands of these applications are rapidly growing. In this context, the data and private information travelling in secure environment to an untrusted environment. In addition of that, the attackers become more equipped and technologically sound. Therefore the traditional

approaches of information security become not much effective. Thus a new kind of mathematical model is required by which the traditional data security schemes are improved.

The proposed work is intended to design and implement a new security algorithm for data cryptography approach. That is based on error diffusion and visual cryptographic approach, which a domain of secret sharing and concept of error filtering. The traditional visual cryptographic scheme is enhanced in such way by which not only image data is encrypted, using the proposed design text data also encrypted using the similar concept.

After analysis and study of different research papers and articles on visual cryptography that is observed there are various different techniques are available to use Visual Cryptography for image encryption. Therefore, visual cryptographic schemes are designed for only image data hiding. Additionally, the classical approaches are used the perception that decryption will be done by the human visual system, but when somebody gets the encrypted shares then it can conceal by stacking the shares and secret image will be compromised. Due to these issues the traditional visual cryptographic schemes are fails in the new era computing. Therefore a new kind of algorithmic process is desired by which the security in image as well as text data can be improved.

In the problem domain two major issues are listed, therefore in order to find the solution of these issues the following suggestions are placed.

1. Extend the traditional cryptographic approach for image and text cryptography: here the traditional cryptographic approach is extended with new features for encrypting image and text approaches.
2. Uses of logical operation in algorithmic process: the whole cryptographic process is synchronized using different logical operations for generating more complex cypher text or data shares.

The cryptographic methodology can be described in two different modules first encryption technique and second the decryption technique. The encryption scheme is given using figure 3 (a) and the decryption scheme is given using figure 3 (b). In encryption scheme the secrete image (half toned image) and data (text or image) is introduced first, after that a Gaussian filter in applied over the data, the filtered half toned image and data is collected after filtering steps. After that an inverter accepts as input both the data and secret key and produces the inverted image and inverted key image. After that step the merging operation is performed over the secret image and the data, the detailed description of the overall merging process is given in figure 3 (a) and figure 3 (b).

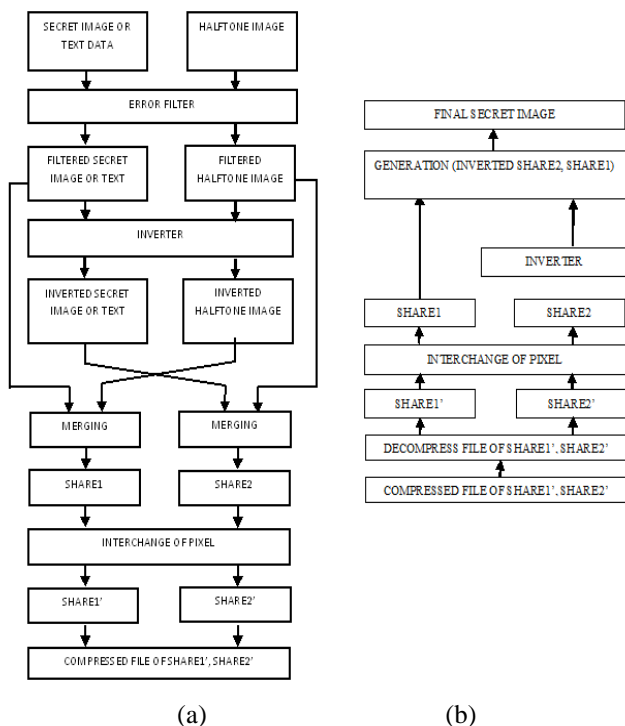


Figure 3 : Cryptographic Scheme

After combining the images two different shares namely share1 and share2 both are treated using the pixel manipulation phase after that two shares are again generated as share1' and share2' compressed share images are encrypted and ready to transfer in network. The revers process (decryption) is provided using the figure 3.1 (b) where the compressed encrypted data is provided as input to the system, and the after that the decompression mechanism is called for recovering the shares. These generated shares are again processed through bit manipulation phase for recovering the original image shares.

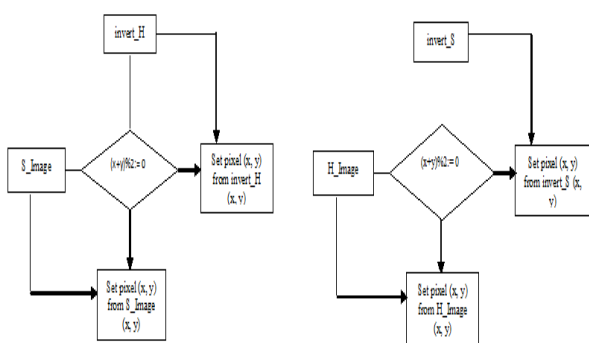


Figure 4 : Merging of Shares

The newly treated data shares are produces into an inverter to obtain the reversely inverted image shares. Those images are then combined for finding the original data. The final combination of generation original message recovery is given using figure 4.

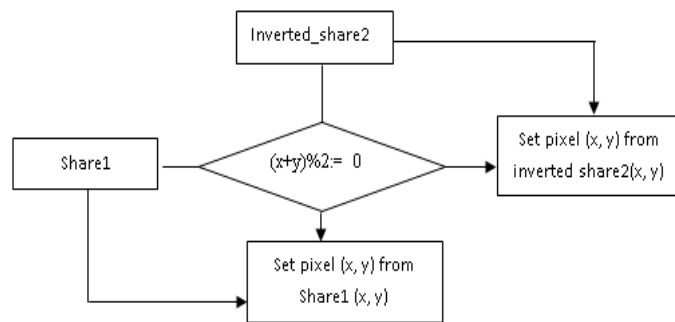


Figure 5 : Original Message Generation

The proposed algorithm can for image and text data encryption and decryption is described in this section.

Input : half toned image (key image), text or image
Output: encrypted image or text
Process: <ol style="list-style-type: none"> <li>1. Select secret data (image or text) and a halftone image.</li> <li>2. Apply error filter for Error Diffusion on secret data and halftone image both.</li> <li>3. Now these filtered secret image or secret text and Halftone image is inverted by inverter.</li> <li>4. Now create shares                         <div style="margin-left: 40px;">                             share1 = merging (invert_H, S_Image)                              share2 = merging (invert_S, H_Image)                         </div> </li> <li>5. for share2 merging (invert_S, H_Image) will be work same as share1</li> <li>6. Now we have two Shares, Share1 and Share2.</li> <li>7. Interchange (share1, share2)                         <div style="margin-left: 40px;">                             repeat for x = 0 to (max width-1)                                  repeat for y= 0 to (max height-1)                                      if ((x+y) %2:=0)  then set share1(x, y) from invert_H (x, y)  else set share1(x, y) from S_Image(x, y)  end if                                      end                                  end                         </div> </li> </ol>

```

Interchange share1(x, y) and share2(x, y)
Else
No interchange
end if
end
end
8. We have two final shares share1' and share2'.
9. Send these shares to receiver using compressed file.
    
```

**Table 1 : Encryption Algorithm**

Proposed decryption technique can be summarized using the table 2.

Input: compressed cypher text
Output: original data
Process: <ol style="list-style-type: none"> <li>1. Get compressed file which have share1' and share2'.</li> <li>2. Interchange(share1', share2')                         <pre> repeat for x = 0 to (max width-1)     repeat for y = 0 to (max height-1)         If ((x+y) % 3:= 0)             Interchange share1'(x, y) and share2'(x, y)         else             No interchange         end if     end end                         </pre> </li> <li>3. Now we have share1 and share2.</li> <li>4. Invert share2 then we find inverted_share2.</li> <li>5. Apply generation (inverted_share2, share1).</li> <li>6. We find the recovered secret image or text data.</li> </ol>

**Table 2 : Proposed Decryption Algorithm**

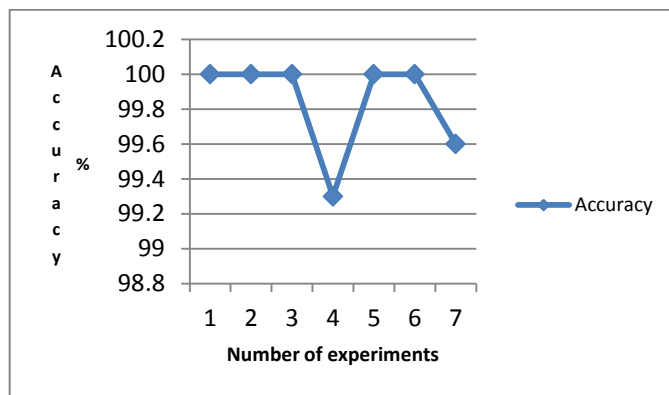
**IV. RESULTS ANALYSIS**

After successfully implementation of the desired technique for image and text cryptography, the performance of the proposed technique is evaluated and listed in this chapter. The performance of the designed system is given using the below given performance parameters.

**A. Cryptographic Accuracy**

Cryptographic accuracy is defined as the percentage of data correctly recovered during the cryptographic process. That can be computed using the below given formula

$$accuracy = \frac{total\ correctly\ extracted\ pixels}{total\ pixels\ in\ original\ file} \times 100$$

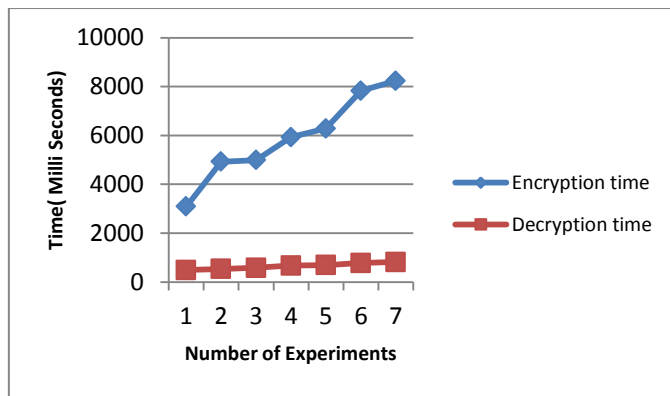


**Figure 6 : Cryptographic Accuracy**

The figure 6 shows the accuracy of cryptographic algorithm during different experimentation. Only first 7 results are placed here for demonstration, here using the change in file formats and file size the performance is provided.

**B. Time Complexity**

The total time required to encrypt and decrypt the files is given here as the time complexity of the system that is provided using figure 7. In this system as the file size increases the amount of time required to encrypt and decrypt is increases accordingly. The below given results are defined in increasing order of the file size during experiments.



**Figure 7 : Time Complexity**

In the above graph the red line shows the decryption time consumption and blue line provides the time complexity of decryption process.

**C. Space Complexity**

The amount of main memory consumed during the encryption and decryption process is given as the space complexity. In

the given figure 8, the encryption and decryption process memory is provided in increasing file size, due to increasing the file size the amount of memory is also increases according to the obtained results.

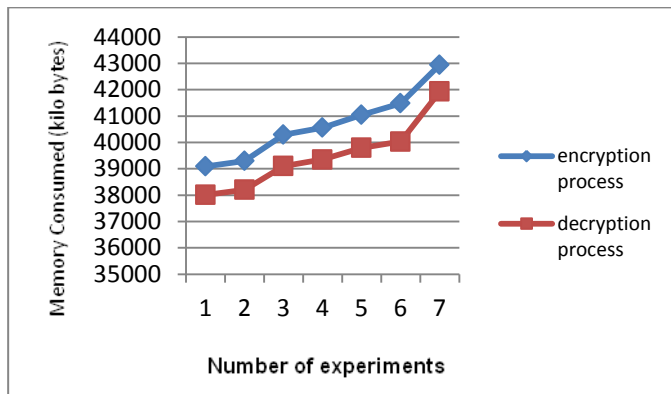


Figure 8 : Space Complexity

V. CONCLUSIONS

Due to the technological development and improvement of computational efficiency the traditional data security techniques are not much appropriate. Due to this new hybrid techniques are discovered for improving the data security. In this context a new encryption technique is implemented for improving the traditional data security. The base concept of the designed algorithm is obtained from the visual cryptography and error diffusion based mathematical model.

The hybrid technique of image and text cryptography is implemented using JAVA technology. Additionally for justifying the proposed methodology the performance in terms of space and time complexity is estimated. The computed performance of the system is summarized using table 3.

S. No	Parameters	Remark
1	Accuracy	The cryptographic accuracy is achieved approximately 100% without any kind of loss in decryption process
2	Time complexity	The time required encrypting an image or text file is always greater than the decryption process. in addition of that as the size of data is increases the amount of time for encryption and decryption process is increases
3	Space complexity	The main memory is also increases as the file size increases in both cases.

		Additionally the memory required to encrypt a file is higher than the decryption process.
--	--	---

Table 3 : Performance Summary

ACKNOWLEDGMENT

The author sincerely thanks, Dissertation guide SHIATS Allahabad, India to carried-out this research work.

REFERENCES

[1] Nitty Sarah Alex, L. JaniAnbarasi, "Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography", 978-1-4244-8679-3/11/\$26.00 ©2011 IEEE

[2] Komal D Patel, SonalBelani, Image Encryption Using Different Techniques: A Review, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011)

[3] DomenicoBloisi and Luca Iocchi, IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY, DipartimentodiInformatica e SistemisticaSapienza University of Rome, Italy

[4] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Robust Hashing for Image Authentication Using Zernike Moments and Local Features, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.8, NO. 1, JANUARY 2013

[5] InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, Color Extended Visual Cryptography Using Error Diffusion, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011

[6] Ch.Samson, V.U.K.Sastry, Encryption of a Gray level Image and a Color Image by Using a Key Bunch Matrix, International Journal of Advanced Computing, ISSN:2051-0845, Vol.46, Issue.2

[7] Wen Chen, Xudong Chen, and Colin J. R. Sheppard, Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain, Received 25 Oct 2011; revised 7 Dec 2011; accepted 3 Jan 2012; published 1 Feb 2012 (C) 2012 OSA 13 February 2012 / Vol. 20, No. 4 / OPTICS EXPRESS 3853

[8] Yu-Chi Chen, GwoboaHorng, and Du-Shiau Tsai, Comment on "Cheating Prevention in Visual Cryptography", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 7, JULY 2012

AUTHOR'S PROFILE



**Shailesh Kumar** belongs to Allahabad. He obtained BTech(CSE) degree from U.P.Tech University, Lucknow in 2009. He is pursuing his M.Tech(CSE) from SHIATS, Allahabad, UP-India. Email: [shailesh.kumar159@gmail.com](mailto:shailesh.kumar159@gmail.com) .

**Er. Archana Singh** belongs to Allahabad. She obtained her M.Tech(IT) degree from SHIATS, Allahabad, UP. India. Presently she is working as Assistant Professor in Computer Science & Information Technology Dept. SSET, SHIATS (Formerly Allahabad Agriculture Institute, Allahabad-India). Email: [archana.singh@shiats.edu.in](mailto:archana.singh@shiats.edu.in)