

# Advance Security for Visual Dataset using Visual Cryptography and Steganography

<sup>1</sup>Gaurang Solanki, <sup>2</sup>Mr. Krunal Panchal

<sup>1</sup>Student, Computer Department, LJIET (GTU), Gujarat, India.

<sup>2</sup>Asst. Prof., PG Department, LJIET (GTU), Gujarat, India.

## ABSTRACT

*In the current technology world, data transmission of various multimedia like sensitive images, video, text is very important and security is major concern in the fields of medical, commercial and military fields. Security is very important, as illegal users may hack the sensitive data. Currently, many techniques are available for Visual data Security. In this proposed system, describes an approach to hide valuable secret information inside the different file formats without losing it by using Steganography and Visual Cryptography techniques. Visual Cryptography is a special kind of cryptographic scheme where the decryption of the encrypted secret is done by the human vision and not by complex mathematical calculations. Visual Cryptography deals with any secrets such as printed or pictures, etc. These secrets are fed into the system in a digital (image) form. The digital form of the secrets is then divided into different parts based on the pixel of the digital secret. These parts are called shares. The shares are then overlapped correctly to visualize the secret. In this method first of all we generate the stego image using cover image and secret data. After that stego image is divide into two shares. This two shares are divided into R,G,B channel and apply 2-level DWT. For scramble the secret data and provide better security we split data into 8\*8 block and then apply inverse 2-level DWT and extract the original secret data. Secret data is hide into the frequency domain of the shares which restrict the various types of attacks and provide better security robustness. Experimental results show that the new scheme is simple and robust.*

**Keywords:** Visual Cryptography, Steganography, Sharing, Multimedia security, Superimposing Images, DWT.

## 1. INTRODUCTION

As there is rise in use of Internet and development in computers in different vicinity of life. Safety of data becomes most important factor in information technology and communication. Information comes in various forms and requires secure communication. For providing secure communication in terms of exchange of information many different methods such as Visual Cryptography, steganography have been developed. Sometime it is not enough to keep the message secret, it may also require to maintain confidentiality and authenticity of the message <sup>[1]</sup>.

Users highly pay attention to the security of their private information. To keep this information secure, two different approaches are used containing cryptography and steganography. Cryptography methods try to encrypt information such that one cannot discover the original information but in steganography, the aim is to deny the existence of a secret message <sup>[2]</sup>.

In steganography, a content or picture is covered up through a media record (e.g. picture) with the end goal that nobody can figure that this document contains whatever other sort of data. At the end of the day, steganography is the specialty of concealing data with the end goal that programmers don't be suspicious to decode or research the record. The concealed content ought to be shrouded to such an extent that the quality and furthermore the statics of that picture don't change. Sending an encode data may draw consideration, while undetectable data won't. In this

manner cryptography is not the best answer for secure interchanges, it is just piece of the arrangement. The execution of steganography can be improved by consolidating it with Visual cryptography. In 1994, Naor and Shamir introduced simple cryptographic method called “Visual Cryptography” (VC) which provides suitable secrecy but it does not have a complex decryption algorithm. Recently, many applications of VC, such as authentication, watermarking, steganography, copyright protection, and visual signature checking have been introduced<sup>[2]</sup>.

## 2. VISUAL CRYPTOGRAPHY

Visual cryptography is the art of encrypting information such as handwritten text, images etc. in such a way that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. The cryptography scheme is given by the following setup. A secret image consists of a collection of black and white pixels. Here each pixel is treated independently. To encode the secret image, we split the original image into  $n$  modified versions (referred as shares) such that each pixel in a share now subdivided into  $n$  black and white sub-pixels. To decode the image, a subset  $S$  of those  $n$  shares are picked and copied on separate transparencies<sup>[10]</sup>.

Since the rise of internet one of the most important factors of important technology is security of Information. Cryptography was created as a technique for securing secrecy of communication and many different methods have been developed to encrypt and decrypt the confidential data. The main goal of secret sharing is to protect important secret data, such as cryptographic keys, from being lost or destroyed without accidental exposure<sup>[2]</sup>.

Visual cryptography schemes were independently introduced by Shamir. Shamir divided data  $D$  into  $n$  pieces such a way that  $D$  is easily reconstructable from any  $k$  pieces, but even complete knowledge of  $k - 1$  pieces reveals absolutely no information about  $D$ . This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces<sup>[10]</sup>.

The first form of visual cryptography is also known as secret sharing. The simplest form of visual cryptography separates a secret into two parts so that either part by itself conveys no information. When these two parts are combined together by means of superimposition, the original secret can be revealed. These parts are called as shares. There are several advantages of visual cryptography. Basically it is simple to use and no mathematical computations are required to reveal the secret. Secondly, the individuals who do not have knowledge of cryptography are indirectly getting involved in decryption. The major drawback of this scheme is that visually blind people cannot make use of this technique<sup>[10]</sup>.

There are number of visual cryptography schemes in existence. Some of them are described below

### A. $K$ out of $K$ Visual Cryptography

Here original secret is divided into  $K$  number of shares and for reconstruction of the secret, all  $K$  shares are necessary. This scheme is not so popular because managing  $k$  number of shares is difficult task and it also increases time complexity to compute shares<sup>[10]</sup>.

### B. $K$ out of $N$ Visual Cryptography

This kind of scheme allows dividing a secret into  $K$  number of shares. Then the secret can be revealed from any  $N$  number of Shares among  $K$ . The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption. The application of this scheme is found with banking system. For the joint accounts, three shares are generated. One is

kept with bank’s server, second is delivered to the one customer for the joint account and third share is delivered to the second customer. Hence both customers are able to access the account <sup>[10]</sup>.

**C. 2 out of 2 Visual Cryptography Scheme**

In this type of visual cryptography scheme, the secret image is divided into exactly two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with remote voting system that uses 2 out of 2 secret sharing schemes for authentication purpose. To reveal the original image, these two shares are required to be stacked together <sup>[10]</sup>. Figure 1 represents the division of black and white pixel in this scheme.

















Pixel	White		Black	
				
Prob.	50%	50%	50%	50%
Share 1				
Share 2				
Stack share 1 & 2				

Figure 1. Basic concept of 2 out of 2 scheme <sup>[10]</sup>

In below visual cryptography example we create two shares (share 1 & share 2) of secret message “WIKIPEDIA”. For getting back original secret message we overlapped this two shares.



Figure 2. Visual cryptography example <sup>[15]</sup>

**3.COMPARISION OF IMPLEMENTED TECHNIQUES**

Table 1 Comparison of Implemented Techniques

NO	PAPER TITLE	METHOD	ADVANTAGE	DISADVANTAGE
1.	Cheating Prevention in Visual Cryptography using Stenographic Scheme.	Secret sharing.  Visual cryptography & Steganography.	Achieve cheating prevention.  Better PSNR value	Partial Cheating creates the confusion between the users about original image.  Doesn't support Priority based VC.

2.	CVC: Chaotic Visual Cryptography to Enhance Steganography.	DCT & DWT based Steganography.  Chaotic map & chaotic function.	Increase the security of hidden messages.  High key sensitivity	Complex.
3.	A Multilayer Visual cryptography Framework for Secured Secret Messages Transmission.	S-DES Encryption Technique.  Visual Cryptography.	Increased the efficiency  Better Security & authentication  The transfer of messages in a more secure manner.	Decryption is slightly complex.  Stego image slices is large.
4.	Hiding Secret Message using Visual Cryptography in Steganography.	DIIVC algorithm (Digital Invisible ink VC)	Unauthorized person can be misguided.  Two levels of security. Useful in military.	Pixel expansion & Contrast loss.  Does not work for complex key.  Seven segment font: Consider 5 & S both are equal.
5.	Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques	Secret sharing.  Visual cryptography & Steganography.	Robust & Simple  High Level Security  Hiding Multimedia Data  Efficiency Increased	Stego Image is hidden in the spatial domain of the vc shares it is prone to transform domain attack.

#### 4. PROPOSED WORK

For enhancing the Security the proposed strategy has been implemented. Below are the Flow diagram and steps for the Proposed System.

Step 1: Take Image.

Step 2: Apply Pre-Processing.

Step 3: Apply Simple Steganography with text and generate Stego Image.

Step 4: Differentiate Stego Image into two share and divide that share into R, G, and B component.

Step 5: Apply 2-level DWT with Cover Image.

Step 6: Split Image in 8\*8 block.

Step 7: Apply Inverse 2-level DWT on every block.

Step 8: Merge all Splitted block and Extract Message.

#### Flow Diagram:

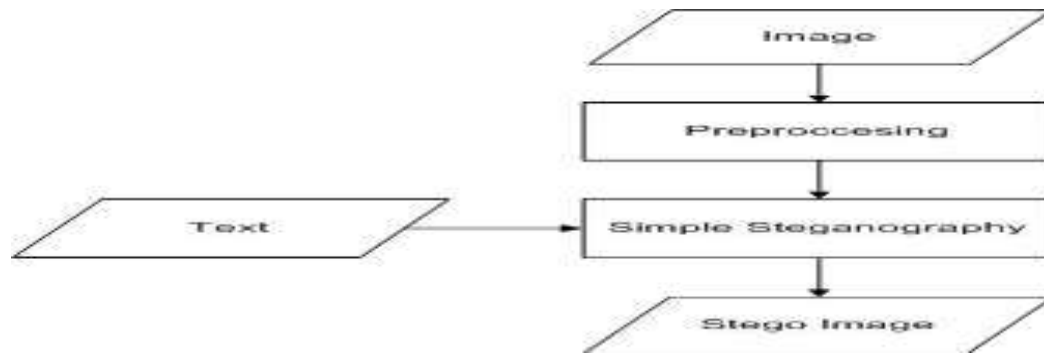


Figure 3. Flow diagram for generating a Stego image

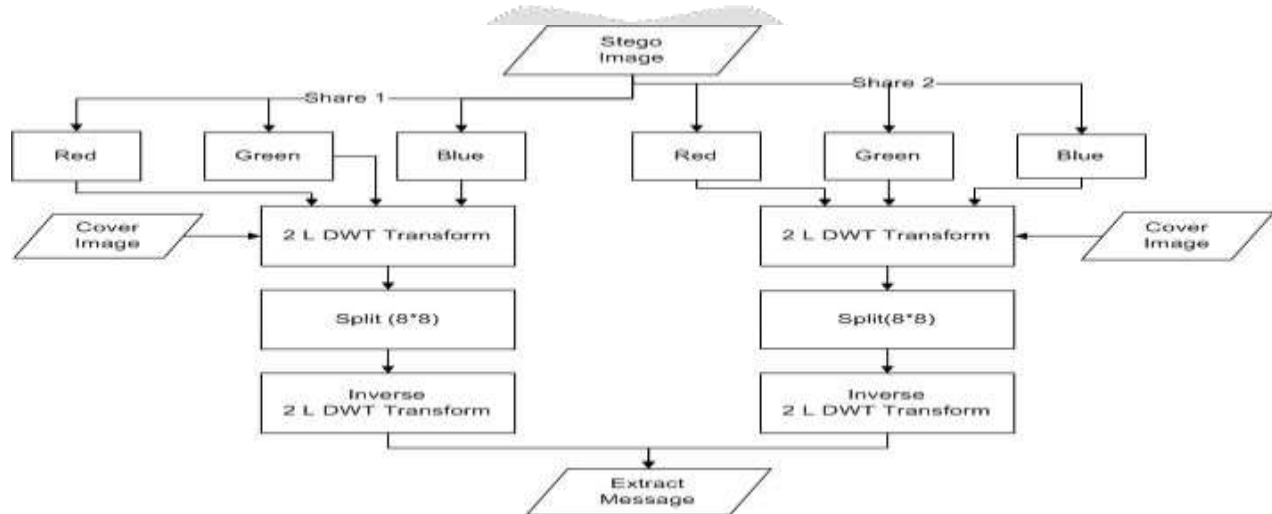


Figure 4. Proposed System Architecture

### 5. RESULT ANALYSIS

For result analysis we implemented proposed system & calculate the PSNR and MSE value. After that we applied different types of attacks like Salt & pepper, Gaussian, Speckle noise, rotate, Blur & unsharp attack and calculate the value of PSNR and MSE. Which shows that our system is robust and provide high level of security.



Figure 5. Cover Image

Figure 6. Secret Image

Figure 7. Stego Image

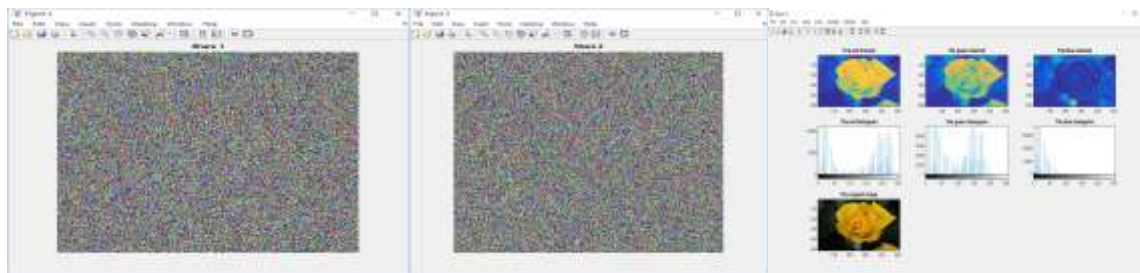


Figure 8. Share 1

Figure 9. Share 2

Figure 10. RGB Channel

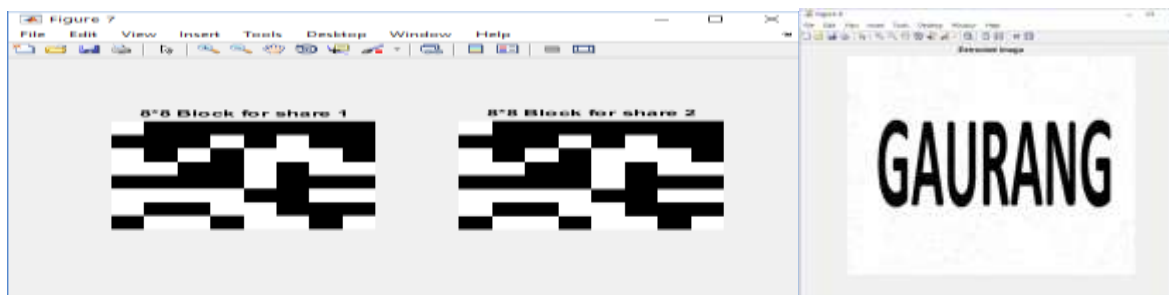


Figure 11. 8\*8 Splitted block

Figure 12. Extracted Image

Table 2. Result analysis without Attacks Table 3. Result analysis with attacks

Secret Image	PSNR(db)	MSE(db)
<b>GAURANG</b>	57.2326	0.1230

Sr.No.	Types of Attacks	PSNR(db)	MSE(db)
1	Salt & Pepper	55.1585	0.1983
2	Gaussian	57.4173	0.1179
3	Speckle Noise	55.6864	0.1756
4	Rotate	57.2415	0.1227
5	Unsharp	56.9687	0.1307
6	Blur	57.2419	0.1227

### 6. CONCLUSION

Based on the literature review the visual cryptography (VC) scheme techniques can decode concealed images without cryptography techniques. The information is hidden by combining the features of both steganography and visual cryptography. According to literature review visual cryptography and steganography is a main technique for data security and authentication. For securing data we use visual cryptography and 2 level DWT transformation with steganography method and also retrieve original data. It is a new way for securing data in images while transmission using the combination of both steganography & visual cryptography. The security of the transformation of hidden data can be obtained by using these two techniques. The Secure data is hidden into the frequency domain which restricts the various types of attacks. Using the proposed system we work on different types of attacks and noise like Gaussian, salt & pepper, speckle, rotate, Unsharp and blur noise to prove our system robust as compared to existing one. Experimental results show that our system is robust. The combination of these two techniques can be used to increase the visual data security.

### REFERENCES

[1] Biswapati Jana, Madhumita Mallick, Partha Chowdhuri, Shyamal Kumar Monda. "Cheating Prevention in Visual Cryptography using Steganographic Scheme." 2014 IEEE: 978-1-4799-2900-9, DOI: 10.1109/ICICICT.2014.6781367, pp. 706-712, 7-8 Feb. 2014.

[2] Melika Mostaghim, Reza Boostani. "CVC: Chaotic Visual Cryptography to Enhance Steganography." 2014 IEEE: 978-1-4799-5383-7, DOI: 10.1109/ISCISC.2014.6994020, pp.44-48, 3-4 Sept. 2014.

- [3] Arghya Ray, A vishake Ghosh, B. Padhmavathi. "A Multilayer Visual cryptography Framework for Secured Secret Messages Transmission." *2015 IEEE*: 978-1-4799-6480-2, DOI: 10.1109/ISCO.2015.7282313, pp. 1-6, 9-10 Jan. 2015.
- [4] Yogesh K. Meghrajani, Himanshu S. Mazumdar. "Hiding Secret Message using Visual Cryptography in Steganography." *2015 IEEE*: 978-1-4673-6540-6, DOI: 10.1109/INDICON.2015.7443677, pp.1-5, 17-20 Dec. 2015.
- [5] Rani, M. Mary Shanthi, G. Germine Mary, and K. Rosemary Euphrasia. "Multilevel Multimedia Security By Integrating Visual Cryptography And Steganography Techniques". *Advances in Intelligent Systems and Computing* (2015), DOI: 10.1007/978-981-10-0251-9\_38 pp. 403-412.
- [6] Sah, Hare Ram and G. Gunasekaran. "Privacy Preserving Data Mining Using Image Slicing And Visual Cryptography". *2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (2015), DOI:10.1109/ICCCNT.2015.7395171, pp.1-7,13-15 July 2015.
- [7] Hodeish, Mahmoud E., Linas Bukauskas, and Vikas T. Humbe. "An Optimal (K,N) Visual Secret Sharing Scheme For Information Security". *Procedia Computer Science*93(2016), DOI: 10.1016/j.procs.2016.07.288, pp.760-767.
- [8] Lee, Cheng-Chi et al. "A New Visual Cryptography With Multi-Level Encoding". *Journal of Visual Languages & Computing* 25.3 (2014), DOI:10.1016/j.jvlc.2013.11.001, pp. 243-250
- [9] Bodke, Minal and j.v. katti. "Reduction Of Transmission Risk Problem In Image Security Using Diverse Image Media". *ScienceDirect* (2016), DOI: 10.1016/j.procs.2016.03.091, pp.875-884.
- [10] Chavan, Pallavi, Mohammad Atique, and Anjali Mahajan. "An Intelligent System For Secured Authentication Using Hierarchical Visual Cryptography-Review". *ACEEE* 02.04 (2011), DOI: 01.IJNS.02.04.525, pp.7-9, Oct.-2011.
- [11] M, Kavita. "Visual Cryptography And Steganography Methods Review". *International Journal on Recent and Innovation Trends in Computing and Communication* 3.4 (2015), DOI:10.17762/ijritcc2321-8169.150437, pp. 1927-1930, April-2015.
- [12] Gayathri, R. and V. Nagarajan. "Secure Data Hiding Using Steganographic Technique With Visual Cryptography And Watermarking Scheme". *2015 International Conference on Communications and Signal Processing (ICCSP)* (2015), DOI:10.1109/ICCSP.2015.7322691, pp. 0118-0123, 12 November 2015.
- [13] Ramya, J. and B. Parvathavarthini. "An Extensive Review on Visual Cryptography Schemes". *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)* (2014), DOI: 10.1109/ICCICCT.2014.6992960, pp.223-228, 22 December 2014.
- [14] "The CIA Principle". *Doc.ic.ac.uk*. N.p., 2016. Web. 6 Nov. 2016, Time: 10:19 AM.
- [15] "Visual Cryptography". *Wikipedia*. N.p., 2016. Web. 24 Aug. 2016, Time:11:52 AM.