

A Survey on Advance Security for Visual Dataset Using Visual Cryptography and Steganography

¹Gaurang Solanki, ²Mr. Krunal Panchal

¹Student, Computer Department, LJJET (GTU), Gujarat, India.

²Asst. Prof., PG Department, LJJET (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. The main objective is to never leave anyone to know that information is already hidden in the file. 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.

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

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 ^[1].

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 ^[2].

In steganography, a text or image is hidden through a media file (e.g. picture) such that no one can guess that this file contains any other type of information. In other words, steganography is the art of hiding information such that hackers do not be suspicious to decrypt or investigate the file. The hidden text should be hidden such that the quality and also the statics of that image do not change. Sending an encrypt information may draw attention, while invisible

information will not. Therefore cryptography is not the best solution for secure communications, it is only part of the solution. The performance of steganography can be enhanced by combining 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^[2].

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^[10].

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^[2].

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^[10].

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^[10].

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^[10].

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 ^[10].

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 ^[10]. 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 ^[10]

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 ^[15]

3.RELATED WORK

3.1 Cheating Prevention in Visual Cryptography using Steganographic Scheme

In this paper ^[1] proposed a stenographic approach to detect fake share and then revealed secret image from original share. Their attacks are to reveal fake images which cheat honest participants. There are two types of cheaters in this scenario. One is a malicious participant (MP) and the other is a malicious outsider (MO).

Stacking the Fake Share with all other share includes S₁ (share), it will show the Fake image, and when stack the Fake Share with all other shares excluding S₁ (share) then show overlapping image of original image and fake image. It is known as Partial Cheating, creates the confusion between the users about original image. This type of cheating is done by a Malicious Participant. Fake share can be detected by checking the message, embedded within it without any verification share. The system can be improved by embedding secret message in column major to different share, so

that we can give the priority to each share. Priority based VC can be used in different organization which can be developed in future.

3.2 Chaotic Visual Cryptography to Enhance Steganography

In this paper ^[2] author proposed a technique to increase the security of hidden messages, visual cryptography can be combined with steganography. In addition, to make the visual cryptography more robust, here, a chaotic function is employed to generate one of the visual components (share). In other words, just one share is sent and the receiver side, the related share is generated and will combine to the received share to reveal the hidden message. The proposed scheme is evaluated in terms of histogram uniformity, has an acceptable correlation coefficient, key sensitivity and key space.

The secret message cannot be correctly decrypted when there is only a very low difference between the encryption or decryption keys. Using visual cryptography not only increases the security level but also does not impose a complex computational burden to the procedure.

3.3 A Multilayer Visual cryptography Framework for Secured Secret Messages Transmission

In this paper ^[3] the proposed model not only strengthens the cryptosystem by integrating random key generation technique using key bunch matrix, and an improved S-DES algorithm but also makes the cryptosystem hard to crack. The generated cipher text is embedded into an image, which is then sliced into a number of parts say 'n' different parts, thereby fully safeguarding the inbuilt secret message.

The secret text can only be interpreted or deciphered when all the slices of the image are securely exchanged between the authorized users and superimposed in the correct order. The proposed crypto system has increased the overall efficiency and strengthened the authentication and security barrier.

3.4 Hiding Secret Message using Visual Cryptography in Steganography

In this paper ^[4] author presents two layered security for data hiding by combining steganography and visual cryptography (VC). Classically, VC encrypts a secret image into noise like images called as shares and decrypts secret message by stacking of shares, whereas steganography hides secret into another image called as cover image, where only intended receiver decodes the message. Steganography often encodes secret message using secret key before hiding into another image. Cover message and encrypted secret message are encoded into noise-like shares using (2,2) VC where concept of digital invisible ink of steganography is incorporated with VC (DIIVC) to hide secret message. Unlike typical steganography, shares are modified to conceal secret message instead of cover image. At receiver, decryption of shares using conventional VC results poor contrast cover image. Result appears as sole secret disclosed using VC whereas only intended receiver has knowledge of secret message. Further, intended receiver retrieves encrypted secret message by applying proposed DIIVC algorithm on resultant cover image. Finally, original secret message is revealed using secret key. The proposed scheme is useful in military, business to send proper secret message to authorized user where it misguides espionage.

3.5 Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques

In this paper ^[5] author proposed a novel approach for multimedia data security by integrating Steganography and Visual Cryptography (VC) with the goal of improving security, reliability and efficiency. The proposed technique consists of two phases. The first phase is used to hide the message dynamically in an Cover Image1 by changing the number of bits hidden in RGB channels based on the indicator value. VC schemes conceal the Cover Image2 into two or more images which are called shares. In the second phase two shares are created from a Cover Image2 and the stego image created in the first phase is hidden in these two shares. The shares are safe as they reveal nothing about the multimedia content. The Cover Image2, stego image and the hidden message can be recovered from the shares without involving any complex computation.

The results prove that the quality of the recovered image and message is same as that of the original image and message. Any digital data can be transferred in a secured way using this scheme. More amount of information can

be transmitted by increasing the number of VC shares. The stego image is hidden in the spatial domain of the VC shares it is prone to transform domain attacks. To overcome, this work can be extended to hide the data in the frequency domain of the shares.

4.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.

5. CONCLUSION

Based on the literature review the visual cryptography (VC) scheme techniques can decode concealed images without cryptography techniques. The information is hiding by combining the features of both steganography

and visual cryptography. According to literature survey visual cryptography and steganography is a main technique for data security and authentication. For securing data we use visual cryptography and DWT transformation with steganography method and also retrieve original data using LSB and MSB embedding or with pseudo random sequence/bit pattern. It is a new way for securing data in images while transmission using the combination of both steganography & visual cryptography. First of all data is hidden in image using steganographic technique then data hidden within images is kept secret using visual cryptography technique. The security of the transformation of hidden data can be obtained by using these two techniques. The combination of these two techniques can be used to increase the data security.

REFERENCES

- [1] Biswapati Iana, 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 (ICCS)* (2015), DOI:10.1109/ICCS.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 (ICICCT)* (2014), DOI: 10.1109/ICICCT.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.

