ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

VISUAL CRYPTOGRAPHY AND STEGANOPGRAPHY: A REVIEW

Radhika R. Raut[*1] and Prashant L. Paikrao[2]
[*1] Student, Department of Electronics Engineering, Government College of Engineering Amravati, India.
[2]Assistant Professor, Department of Electronics Engineering, Government College of Engineering, Amravati, India.

Keywords: Cryptography, Steganography, Ciphertext, Plaintext, Public Key, Private Key, Halftone Image

ABSTRACT
Information sharing and transmission is increasing day by day, information gets more value when shared. Due to rapid development in networking and communication technologies, it became easy to share the multimedia information. It may give rise to security related issues. Attackers may try to access the information and misuse it. To address this problem certain techniques are required to increase security.

Visual cryptography (VC) is a technique used for protecting secrets using images, Visual Cryptography is an encryption technique used to hide information in an image in such way that only those can decrypt the images who has secret key. The basic concept of visual cryptography scheme is, to split secret image into some shares. Shares are then distributed to receiver side. By stacking these shares directly, secret information can be revealed and visually recognized by authorized person. Steganography is an art, science or practice in which messages, images or files are hidden inside other messages, images or files. All shares are necessary to combine to reveal the secret image. Starting from the basic techniques, many visual cryptographic techniques have been developed.

INTRODUCTION
Steganography is the art and science of encoding a secret message into images in such a way that only the sender and intended receiver are aware of its existence. Cryptography is algorithm of enciphering and deciphering the data and information with a secret key.Thus protecting this data in a safeand secure way which has security against unauthorized attacks.

Many attempts have been madeto solve this problem in data hiding.Images do not convey any significantinformation and they can be used to hide a secret message.Also, some pixels of the image can be modified to carry asmall modification such as leastsignificant bit of pixels. For confidential war plans, stealthy military data, web based applications, there must be protection of the digital image. So there is need to have techniques to secure confidential data to increase security and protection against unauthorized person.

By combining the features as well as advantages ofboth the techniques, visual cryptography and Steganography in images is introduced. Visualcryptography provides a very powerful technique by whichone image can be distributed into two or more shares.When the shares are reassembled exactly together, theoriginal image can be revealed. Pixelexpansion and low contrast of the recovered image is the mostimportant drawback in visual cryptography.
There are mainly two types of basic cryptographic algorithms: symmetric and asymmetric algorithms. Symmetric systems such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) use an identical key for the sender and receiver; both to encrypt the message text and decrypt the cipher text. Figure 1 and 2 shows Public key cryptography and joint key cryptography.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

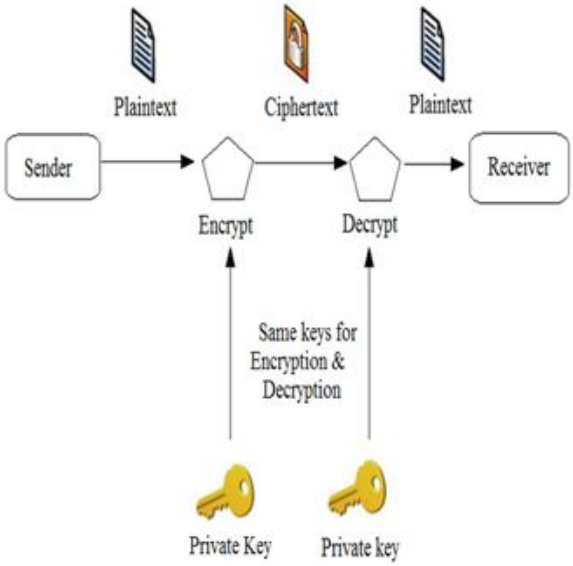

Fig. 1. PrivateKey cryptography

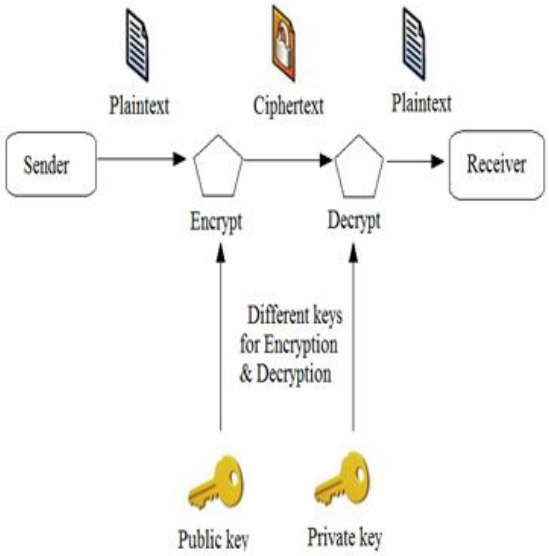

Fig. 2. Public Key cryptography

PRIVATE KEY CRYPTOGRAPHY (Symmetric key cipher) uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. Joint key cipher algorithms are less complex and execute faster as compared to other forms of cryptography but have an additional need to securely share the key. In this type of cryptography the security of data is equal to the security of the key.

PUBLIC KEY CRYPTOGRAPHY (asymmetric key cipher) is a technique that uses twodifferent keys– a public key and a private key (secret key) for encryption and decryption. The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key. This technique eliminates the need to privately share a key as in case of symmetric key cipher. Asymmetric cryptography is comparatively slower but more secure than symmetric cryptography technique.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

Asymmetric systems such as Rivets-Shamir-Adelman & Elliptic Curve Cryptosystem use different secret keys for encryption as well as decryption. Symmetric cryptosystems is more suitable to encrypt large amount of data with high speed. In 1995, Naor and Shamir introduced a basic cryptography algorithm.To replace the old Data Encryption Standard, in September 12 of 1997, the National Institute of Standard and Technology (NIST) proposed Advanced Encryption Standard (AES). On October 2nd 2000, NIST has announced the Rijndael Algorithm which is the best in security, performance, efficiency, implement ability & flexibility.

At Leuven, Rijndael algorithm was created by Joan Daemen of Proton World International and Vincent Rijmen of Katholieke University. AES encryption technique is an efficient scheme for both hardware and software implementation. As compare to software implementation of these techniques, hardware implementation provides greater physical security and higher speed. As new algorithms are implemented, numerous techniques are developed for encryption.

In 2007, simple cryptography and Steganography based paper is published named as Visual cryptographic Steganography in images. In this paper basic algorithm is explained used to increase the security on web based applications. The algorithm also is more secure than a normal cryptographic system as the encrypted data is hidden into a multimedia file and then transmitted.It is also more secure than a Steganography system as the data to be hidden is in an encryptedformat. The algorithm scores over traditional visual Steganography systems like LSB encoding[1].

Next paper presented on cryptography was Steganography and visual cryptography incomputer forensics in 2010. Different algorithms for Steganography and visual cryptographyhave different advantages as well as disadvantages and weaknesses. But generally, the job offorensic and security investigators is not easy. When Steganography and visual cryptographydetection tools are used together, then it is almost impossible for hackers to uncover hidden orencrypted data. If both techniques are used, then it makes investigators much easier and givesthem a better chance of detecting suspicious data [2].

Another technique discussed in Digital image chaotic encryption in 2014. Using blocklevel encryption for images was used help to overcome correlation between neighboring pixels,which is main feature used in image encryption. The block size should be smaller for bettertransformation because only fewer pixels will keep their neighbor's data. In this new blockcryptosystem for encoding images named as Digital Image Chaotic Encryption (DICE) has been discussed [3].

Next technique was Privacy preserving data mining using image slicing & visualcryptography presented in 2015. In this technique Slicing geometry (image) into different framesand encrypting them can help in hiding a secret message within the image and also preserveprivacy of image. Authenticated users can use that relevant key and extract the original image atits destination. This called as visual cryptography or Steganography is one of the most secureforms of message transferring techniques available today which is highly suited for image files[4].

Next to this was Pixel swapping and parity based image Steganography which ispresented in 2016, the part of information is encrypted in the carrier in such way that it is notperceptible to the unauthorized person. In cryptography, the message is converted to make itdifficult so that it becomes a difficult to crack even for experts. This technique based on parityand substitution for gray scale and color image. It has numerous advantages compare to otherstechniques. For steganalysis, this scheme used visual attack, LSB plane attack, machine learningtechnique and X2 test.

In this method, the image is sliced and randomized, the stored random slices upon matchwith a search string (query), and the original image is retrieved at output side. This method isadvantageous to store large number of records in offices, categorized into different groups, andeach group indexed with specific keys and when used at the receiving side the particular groupimage(s) becomes accessible [5].

Protection of digital images during transmission becomes a serious concern when they areconfidential war plans, top secret weapons photographs, stealthy military data and surreptitiousarchitectural designs of financial

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

buildings, etc. One interesting visual cryptography method isthe (t, n) Threshold Image Hiding Scheme. In this method a secret image hides into 'n' number ofcover images, and can be recovered if's' number of cover images are available. For encryptionthis method uses Lagrange interpolating polynomial, MD5 hashing, and RSA signature to hidethe images [6].

Another visual cryptography algorithm is the Image Size Invariant Visual Cryptography.This method hides two-tone secret image and splits them into binary transparencies. Once thosetransparencies are stacked on top of each other, the secret image is revealed. The secret imagecan also be reconstructed by XOR computations of the transparencies. This algorithm is based onthe conventional VSS (Visual Secret Sharing) method [7].

To improve security another visual cryptography algorithm is the Joint Visualcryptography and Watermarking method which uses the concept of watermarking and visualcryptography jointly [8]. Since the DHCED (Data Hiding in Halftone Image by Conjugate ErrorDiffusion) method cannot prevent the secret image from being extracted with only one of theshares, this method overcome that issue [9]. An interesting point of this algorithm is that it doesnot reveal the secret information even if one has the original image and one of the shares; bothshares have to be present to reveal the secret image.
Next was the Region Incrementing Visual Cryptography method is discussed. In RIVC,the original image is divided into 'n' number of secrets and then 'n+1' number of shares is thencreated. Any 'n' number of 27 shares stacked would reveal 'n-1' number of secrets. Theadvantage of this method is that a user can pick which region of the secret image to assign to asecrecy level which makes it flexible and accommodating to user preferences. As this methodmay not seem to be as secure as other methods because if one has the original image and one ofthe shares; both shares have to be present to reveal the secret image [10].

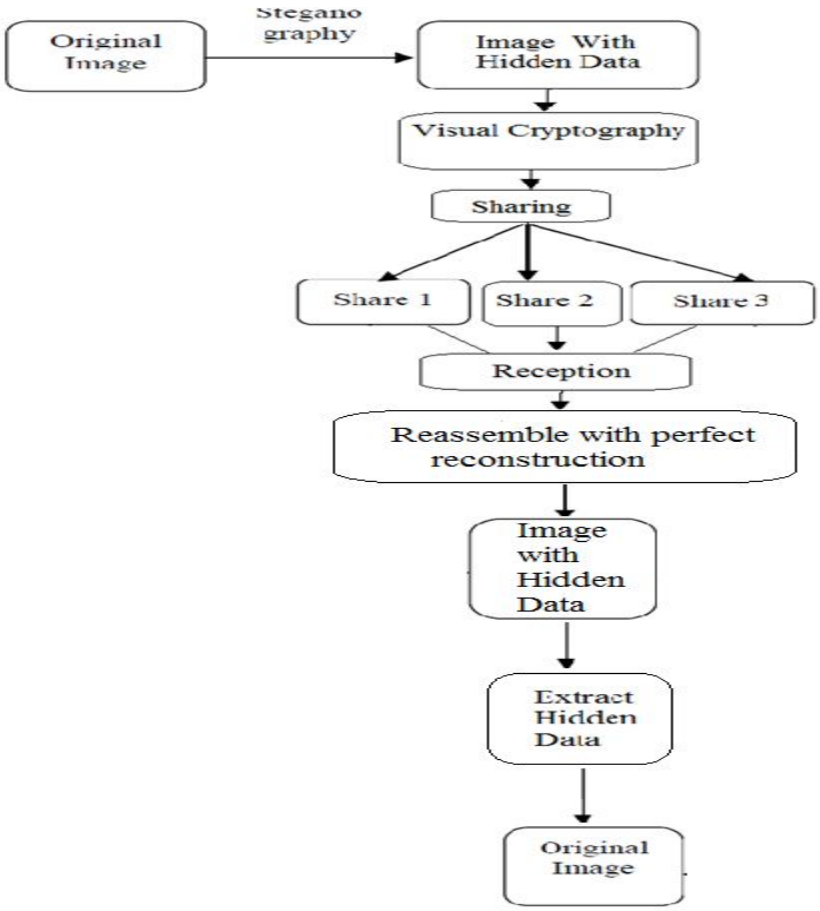

Fig. 3. Proposed Method using both Visual Cryptography and Steganography

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

The proposed technique is a new way for securing data in images while transmission using the combination of both Steganography and visual cryptography. First of all data is hided in color 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. Fig. 3.Shows Proposed Method using both Visual Cryptography and Steganography in images.

CONCLUSION

A data security scheme consists of cryptography and visual Steganography is discussed here. The visual cryptography and Steganography can be implemented using OpenCV tools and hence there are no proprietary issues.

In this method, the definitions of Steganography and visual cryptography have been discussed along with several studies done on various algorithms of each type. Steganography and visual cryptography have many similarities and differences, and thus have various uses in the digital and real world.

There are different algorithms for Steganography and visual cryptography has different advantages and power, as well as disadvantages and weaknesses. So it is found that notice that certain methods are easier to detect than others. Generally, some techniques are not that much amount of security which user wants. When Steganography and visual cryptography detection tools are used exclusively, it is almost impossible for unauthorized to recover hidden or encrypted data.

It noticed that using an algorithm with a reconstruction method will allowsreconstructing shares back into the original image. It would be very interesting to learn howdetectable data is after applying visual cryptography with perfect reconstruction to an image with hidden data

ACKNOWLEDGEMENTS

I would like to thanks my Guide, GCOEA institution and department of Electronics for their full support, guidance, comments and suggestions.

REFERENCES

1. *P. Marwha, P. Marwha, "Visual Cryptographic Steganography in Images", International conference on computing and networking Technologies, 2010.*
2. *G. Abboud, J. Marean, "Steganography and Visual Cryptography in Computer Forensics", Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010, pp 25-32.*
3. *C. Patel, K. Wandra, S. Shah, Digital Image Chaotic Encryption, International Conference on Reliability, Optimization and Information Technology (ICROIT), Feb 6-8 2014.*
4. *H.Sah, Dr. G.Gunasekaran, "Privacy Preserving Data Mining using Image Slicing and Visual Cryptography", 6th International Conference of Computing ,July 2015.*
5. *C. Patel, Dr. K. Wandra, "Pixel Swapping and Parity Based Image Steganography Algorithm", IEEE Students' Conference on Electrical, Electronics and Computer Science, Feb 2016.*
6. *C. Chin-Chen and L. Iuon-Chang, "A new (t, n) threshold image hiding scheme for sharing a secret color image," International Conference onCommunication Technology Proceedings, 2003, pp. 196-202 vol.1.*
7. *L. Hao and Y. Faxin, "Data Hiding in Image Size Invariant Visual Cryptography", 3rd International ConferenceInnovative Computing Information and Control, 2008, pp. 20-25.*
8. *F. Ming Sun and O. C. Au, "Data hiding in halftone images by conjugate error diffusion," International Symposium on Circuits and Systems, 2003, pp. II-920-II-923 vol.2.*
9. *F. Ming Sun and O. C. Au, "Joint visual cryptography and watermarking",International Conference on Multimedia and Expo, 2004, pp. 975-978 Vol.2.*
10. *W. Ran-Zan, "Region Incrementing Visual Cryptography," Signal Processing Letters, IEEE, vol. 16, pp. 659-662, 2009. Reassemble.*