ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Integration of Visual Cryptography and Steganography for Enhanced Security and Confidentiality

Kavita M. Tambe[1] , Ramling D. Patane[2]

PG Scholar, Dept. of Electronics and Telecommunication, Alamuri Ratnamala Institute of Engineering & Technology Mumbai, India[1] ,

Associate Professor, Dept. of Electronics and Telecommunication Terna Engineering College Nerul , Navi Mumbai, India [2]

ABSTRACT: In this paper we have proposed the method for providing double layer of security to the user data. in this method each character of the user data including special character is converted into correspond bit binary numbering ASCII code and then each value is get converted into 8 bit binary number. For embedding process each bit of the character is get embedded into the least significant bit of each pixel of cover image. As only last bit of the each pixel is getting changed, the stego image becomes indistinguishable from the original image.

KEYWORDS:Visual Cryptography ;Steganography; Least Significant Steganography; Stego image ; Cover Image ;Peak Signal to Noise Ration (PSNR); Mean Square Error (MSE)

I. INTRODUCTION

Security of the information is consider as one of the most important factor in today's era of information technology .today Various techniques of information hiding receives much attention .For providing security cryptography was created. sometimes it is not enough only to maintain the security of the information but it becomes important to keep presence of the message secrete, and for this reason steganography comes in to implementation. The Greek word stego precisely means "covered writing"[1].Steganography hides presence of communication where as in cryptography opponent is allowed to detect , intercept and modify the message without breaking certain security premises guaranteed by a cryptosystem. The main aim of steganography is to hide message inside the other message in such a way that the enemy will not even detect the presence of the hidden message .All the digital files format can be used with the steganography but the formats with the high degree of redundancy becomes more suitable. Redundancy is defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant can be altered and the alteration cannot be easily get detected. Steganography can be performed on text, image audio files but an Image and audio file completely fulfils the requirement of redundancy for information hiding. Visual Cryptography is a method used for encrypting a secret image into shares, in a such way that after stacking the shares it reveals the secret image. To add multiple layers of security it is a good practice to use Cryptography and Steganography together. Neither cryptography nor Steganography are considered "turnkey solutions" to open systems privacy, but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

II. STEGANOGRAPHIC METHODS

There are three different approaches that can be used to hide information in a cover object:

1. Injection: Hides the secret message into the host medium
2. Substitution : Replace the bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion
3. Generation: Generation of new files.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

III. STEGANOGRAPHIC TECHNIQUES

A. *The different categories of Steganography techniques are :*

- Substitution system techniques
- Transform domain techniques
- Spread spectrum technique
- Distortion techniques
- Statistical method techniques

B. *Steganography techniques can be broadly classified as*

- Spatial domain techniques
- Transform domain techniques
- Hybrid domain techniques

IV. VISUAL CRYPTOGRAPHY

It is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without help of computers.[2] It was proposed by Naor and Shamir in 1994[3]. The secret information may be handwritten notes, images or text that can be uncovered without any complex cryptographic computations [3]. In (k,n) visual cryptographic scheme , the secret information can be divided into k shares and shared among n participants . The information can be recovered if k or more shares stacked together. If the number of shares are (k-1) or less than that then it is not possible to reveal the information.

V. CRYSTOGRAPHY-COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography and steganography are cousins in the spy craft family; the previous one scrambles a message so it cannot be understood, the latter hides the message so it cannot be seen. Basically, the purpose of Steganography is not the same as cryptography. Data hiding techniques have been widely used to transmission of hiding secret message for long time. Information security and confidentiality is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together [4] . The combination of these two methods will enhance the security of the embedded data. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

As an independent method both steganography and visual cryptography have problems and provide only single layer of security which can be easily broken by intrude[11]r. Combing features of both the technique provides double layer of security.

VI. METHODOLOGY USED

Many techniques can be used for implementing combinational approach of steganography and visual cryptography .In this paper we describe LSB Technique for embedding text into the image.

A. *Data Embedding and image slicing Procedure:*

The secrete message is first converted into the equivalent ASCII characters and then into binary digits. For example if the character is “t” then its ASCII vale is 116 and the corresponding binary value will be 1110100.An image is an array of pixels.

Every pixel has numbers from color components – for 24 bit bitmap image each red , green and blue pixel has 8 bits. In 8 bit of color number, if we change least significant bits then our visual system cannot detect changes. Changing LSB of the pixel is nothing but adding or subtracting one from the pixel value it represents.

Suppose our original pixel has bits:

(r7 r6 r5 r4 r3 r2 r1 r0, g7 g6 g5 g4 g3 g2 g1 g0, b7 b6 b5 b4 b3 b2 b1 b0)

In addition, our character has some bits: (c7 c6 c5 c4 c3 c2 c1 c0).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Then we can place the character bits in the least significant of selected pixel, next character bits in the next lowest pixel, and so on.

(r7 r6 r5 r4 r3 r2 r1 c2, g7 g6 g5 g4 g3 g2 g1 c1, b7 b6 b5 b4 b3b2 b1 c0).

If we take an example of pixel (225,107,100) represented in binary form (11100001, 01101011, 01100100) into which to embed message character "a" having bit 01100001(ASCII value 97), then we can obtain New pixel as (224, 106,101) represented in binary form (11100000, 01101011, 01100101).

Here we can notice that a pixel value of (225,107,100) is changed to a new pixel value of (224,106,101). This change is not visible to human vision. Once all the message characters are embedded into the cover-image, the target character zero is inserted in the pixel of the cover-image immediately. The target character is known as Terminator Character.

In the slicing process of visual cryptography the image get slice into multiple numbers of shares. The generated shares reveals no information about the secrete message.

B. *Data Extraction and share Stacking Procedure*

After receiving the slides (shares) all the shares get stack on each other to form master slide which contains the secrete message . If the numbers of shares are less then it is not possible to reveal the information. In the image based steganography Stego image is used for exacting the secret information. The extraction of secrete message is called as Steganalysis. The data extraction procedure is opposite of embedding procedure.

In extracting the message, the process opens the stego-image file and read the RGB color of each pixel. The LSBs of each pixel of stego-image is extracted. As in the embedding process a Terminator (Target) Character is placed in the message which is the last character to signify the end of embedding of data. When the binary representation of the Terminator character is found the extraction process stops. Thus the terminator character helps the extracting algorithm to stop reading the bits of the stego-image from next pixel onwards as no more data is embedded in further pixels. The bits of the LSB are retrieved and placed in the array. Then content of the array converts into decimal value that is actually ASCII value of message.

VII. ANALYSIS AND RESULTS

Fig.1. Cover Image

Fig. 2.Stegao Image

The proposed method provides high levels of security as it uses double security level by combining steganography and visual cryptography. In the experiment we observed that the messages were successfully hide into the cover images. The complexity of the image is not disturbed as shown in figure 1and figure 2. The difference of the cover image and stego-image can hardly be distinguished after using the LSB method insertion.

After slicing, stacking and decoding the embedded information can be successfully retrieved.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

VIII. PEAK – SIGNAL-TO –NOISE RATIO[PSNR]

Visual Quality of the covering image can be measured by a numerical quantity termed as Peak Signal-to-Noise Ratio (PSNR) and it is given as[5][10] :

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

In calculation of PSNR the cover image is the original image and error introduced by compression is consider as noise. PSNR is measured in terms of dB. higher the value of PSNR , higher the quality of reconstructed image .Mean Squared Error (MSE) is used for calculation of PSNR.

TABLE I. PSNR AND MSE VALUES OF IMAGES

Cover image	Stego Image	MSE %	PSNR (dB)
Cat	Stego cat	0.0358	62.62
Flower	Stego flower	0.0352	65.23
Marbles	Stego marbles	0.366	62.59

When there is increase in the payload, then MSE also gets increased and PSNR gets decreased. If the value of PSNR is below 30 dB then Quality of image is low, where as if the PSNR is above 40 dB them image quality is high and less distortion caused by the embedding process[7][8][9]. From the table we can observed that all the three images used have high value of PSNR which indicates that quality degradation could hardly be notice by a human eye.

IX. CONCLUSION

As many people depend on the internet for sharing information, the need for information security is also gets increased. This paper describes LSB steganographic method for hiding the text data into the color image and then using the visual cryptography for proving double level of security. Bothe steganography and visual cryptography have their own drawback but combination of both the technique becomes more immune to the unauthorized access to the secrete information The proposed technique shows promising results as shown in Table 1 and figure 1 and 2 .

REFERENCES

1. Shamim Ahmed LaskarandKattamanchiHemachandran , “High Capacity data hiding using LSB Steganography and Encryption” , International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.
2. Vipul Sharma , Sunny Kumar , “ A New Approach to Hide Text in Images Using Steganography” , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013 ISSN: 2277 128X.
3. NavneetKaur, Sunny Behal, “A Survey on various types of Steganography and Analysis of Hiding Techniques”, International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014
4. Avcibas, I., Memon, N., and Sankur, B. ; “ Steganalysis Using Image Quality Metrics”, IEEE Transactions on Image Processing, Vol. 12, No. 2, pp 221-229, 2003.
5. S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O. Gorman, “Document marking and identification using both line and word shifting,” INFOCOM’95 Proceedings of the Fourteenth Annual Joint Conf. of the IEEE Computer and Communication Societies, 1995, pp. 853-860.
6. Jerripothula Sandeep, Abdul Majeed. “Embedded Extended Visual Cryptography Scheme”, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 8, Issue 1 (Nov. - Dec. 2012), PP 41-47
7. GunjanChugh, “IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE” , ACTA TechnicaCorviniensis-Bulletine of Engineering Tome VI (Year 2013)-FASCICULE 3 [July-September] ISSN 2067-3809
8. Bret Dunbar, “A detailed look at Steganographic Techniques and their use in an Open- Systems Environment”, SANS Institute InfoSec Reading Room, SANS Institute 2002.
9. Monish Kumar DuttaAsokeNath, “Scope and Challenges in Visual Cryptography”, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 11 (November 2014).
10. An overview of image steganography by T. Morkel , J.H.P. Elo_, M.S. Olivier.Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

11. Anderson , R. J. and Petitcolas, F. A.P. (1998) "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, Vol.16 No.4, pp.474-481, ISSN 0733-8716.

BIOGRAPHY

Kavita M. Tambe pursuing her M. E. in Electronics and Telecommunication Engineering from University of Mumbai. Life member of Indian Society for Technical Education (ISTE) and The Institute of Electronics and Telecommunication Engineers (IETE) from 2015.

Ramling D. Patane is Associate in Terna Engineering College Nerul , Navi Mumbai, under the department of Electronics and Telecommunication. Guide many PG scholars. More than 15 Years of teaching experience