

# A Survey on data conceal and protection in digital image

Neeraj Yogi<sup>1</sup>, Prof. Shweta Shrivastava<sup>2</sup>, Dr. Vineet Richhariya<sup>3</sup>

<sup>1</sup>Student, M.Tech. (CSE), LNCT Bhopal, Madhya Pradesh, India

<sup>2</sup>Assistant Professor (CSE), LNCT Bhopal, Madhya Pradesh, India

<sup>3</sup>Head of Department (CSE), LNCT Bhopal, Madhya Pradesh, India

\*\*\*

**Abstract** – In present scenario internet is growing into a more important part of data transfer for communication. Today internet transfers lots of data in every second and most of the time the data that transfers through internet is confidential, vital and private information. Any communication of internet application and network application needs security. Data security on internet became major concern for where vital information needs to be send and concealed from outer world. Steganography and cryptography are two techniques used for data security in the last decade. Steganography hides information in other media and cryptography converts information in unreadable form. Lots of data security and data hiding algorithm have been developed in steganography and cryptography. In this paper we suggested a few techniques in which steganography and cryptography with compression used to achieve higher level security for transmitting information.

**Key Words:** vital information, security, Image steganography, Cryptography, Compression.

## 1. INTRODUCTION

Today internet turned into great media to transfer and share data like audio, video, text, etc. across the globe. Information transmission over the internet is growing at a rapid rate along with some sensible data like as email, message, credit card information and corporate data, however growing data transfer have brought new risks, such as hacking and its misuse makes data security become a major concern. The Internet domain is changed into personal and private domains. This creates need to provide protection and security to the secret data being transmitted through the Internet. Many techniques developed for providing security to confidential data over the internet. Steganography and cryptography are widely used techniques to provide secure transmission. Steganography and cryptography is a part of information security.

Cryptography is not sufficient for hiding data alone and cannot protect data efficiently. Encrypted data can be easily suspected. For any eavesdropper can detect easily presence of secret data so he can try many attack on encrypted data to retrieve original information. Further enhancement in data security can use steganography. Compression can also reduce actual information.

Combination of Steganography and cryptography with data compression technique can provide higher security.

## 1.1 Image steganography

Steganography is technique to hiding data into media that means covered writing or steganography is an art for hiding data [18,2]. Cryptography converts message in scramble form and it can't be understood. This paper suggested a new system in which compression is used with steganography and cryptography for achieving higher security, confidentiality from outer world.

### 1.1.2 Terms used in steganography

- **Cover image:** In Steganography image is used as carrier for hidden information.
- **Message (data):** Message is the actual information. Message could be plain text or some other image that hide into cover image.
- **Stago image:** stago image is embedding message into cover image.
- **Stago key:** key is used for embedding and extracting message from cover image.

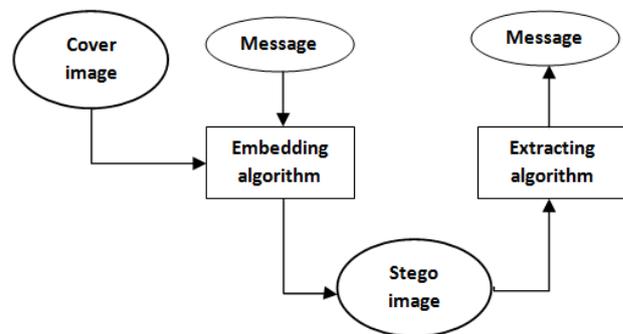


Figure 1.Data hiding in Steganography

Steganography's main objective is data hiding, which nobody should figure out what data embedded in image. On the other hand cryptography converts data in some other form that can't be understood by anyone. Image steganography can be classified in two types:

1. Spatial domain
2. Frequency domain.

- **Spatial domain:** In spatial domain steganography secret message is directly embedded in pixels.
- **Frequency domain:** In frequency domain images are converted into frequency domain and then the secret data is embedded in the transform coefficients [14].

### 1.2 Cryptography

Cryptography is method of transmitting data in particular form so that those for whom it is intended can read and process it. Cryptography divided in two part encryption and decryption. Information converts into unintelligible form this process known as encryption and to get back the original information from encrypted information, this process known as decryption. Data should get in original form after decryption.

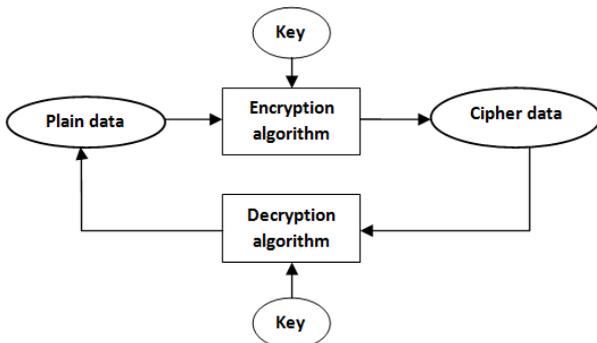


Figure 2. Encryption and Decryption process

The encryption algorithm can be divided into two types based on using key.

1. Symmetric key
  2. Asymmetric key
- **Symmetric key:** In symmetric key encryption algorithm uses same key for encryption and decryption.
  - **Asymmetric key:** In asymmetric key encryption algorithm uses more than one key, it uses different key for encryption and decryption.

Asymmetric key algorithm has very higher computation costs data. Symmetric key algorithm has lower cost [11].

### 1.3 Data compression

There is a possibility that the intruder can break the code, this type of possibility can be removed at maximum level. It is best way to insert compressed data into cover image directly instead of direct data insert into cover image. Compression converts larger size data into smaller size data. Compression is a reduction in the numbers of bits of data. Compression can be lossless or lossy. In lossy data compression technique after compression, removes some part of data. In lossless compression after compression, decompression can achieve same data [21].



Figure 3. Data compression process

There are many lossless compression techniques proposed, some of main techniques –

- Huffman coding
- Run length encoding
- Arithmetic encoding
- Dictionary based encoding

### 2. LITERATURE SURVEY

[3,21] Anil Khurana, B. Mohit Mehta and S. Walton proposed that in image Steganography various methods have proposed for data (message) hiding in images during the last decade. An image can hide number of bit in each pixel. Secret data bit can hide in Least Significant Bit (LSB) and Most Significant Bit (MSB). This paper describes two ways of data hiding in image are LSB and MSB.

LSB (Least Significant Bit): In this method least significant bit of each pixel of cover image is used to embedding message.

MSB (Most Significant Bit): In this method most significant bit of each pixel of cover image is used to embedding message.

[22] L. F. Turner showed a method of pseudo-random number generation to get the security indigital material. Select digital word by digital material and selection of word by independently. Least significant bit of selected word changed.

[15] D. C. Wu and W. H. Tsai proposed an efficient steganography method for embedding message into gray color image. Cover image is partitioned into blocks of two consecutive pixel and blocks is not overlapping to each other. A difference value is found out with help of two pixels of each block. All difference value divided into a number of ranges. Interval of range is selected based on the characteristics of human vision’s sensitivity. The difference value is replaced by new value to embed the value of sub stream of message. The width of range is decided the number of bit can be embedded in a pixel pair.

[10] C. M. Wang and N. I. Wu proposed a pixel value differencing technique and the modulus function. First calculate difference of two consecutive pixels and then calculate remainder of two consecutive pixels by modulus function. Secret message can be embedded into modifying the remainder of two pixels. This method focused on reduced image distortion due embedding secret message.

[5] C. H. Yang and C. Y. Weng proposed a pixel value differencing technique embedded data by changing the difference value of two consecutive pixels. Modification of difference value is used to increase embedding capacity. It is method for searching edge area more flexibly by finding pixels of edge area. In addition shifting scheme is used to further increase change for embedding data.

[12] H. C. Wu and N. I. Wu proposed a novel steganographic method based on LSB substitution method and PVD method

to improve hiding bits in image. To hiding secret bit in cover image this method divided into two parts in first part search smooth area and hiding bit by LSB method. In second part method is searching edge area and hiding bit by pixel value differencing method.

[11] C. H. Yang, C. Y. Weng proposed an adaptive LSB method and PVD method in which showed how many bits can hide in image into two pixels. In this range of difference values is divided into lower level, middle level, and higher level. Number of bit to be embedded is decided by the level in which the difference value lies.

[6] X. Liao, Q. Y. Wen, and J. Zhang proposed a 4 pixels differencing and modified LSB substitution methods to hide secret bits. Number of bit to be embedded is decided by the level in which the difference value lies.

[13, 7] Chang and Tseng is used a data substitution method based on the side match for two sided, three sided and four sided. T. J. Ross showed a fuzzy theory that helps for data hiding.

[1] Masume Sabokdast, Majid Mohammadi proposed a fuzzy system with 4 pixels differencing and modified LSB substitution method for hiding data bit into image. Number of bits for hiding is calculated by fuzzy systems.

Encryption uses for gain higher security it converts data into another form.

[14, 16] W. Stallings showed various methods for text encryption such as DES, AES, RSA and IDEA. Higher security can achieve by DES, AES, RSA and IDEA. All these methods are for text encryption only not for image and video. M. V. Droogenbroech and R. Benedett showed Encryption on image needs special requirements and thus requiring different encryption algorithms.

[17] Jiun-In Guo, Jui-Cheng Yen described various methods for image encryption such as position permutation based algorithm, value transformation based algorithm and transformation based algorithm.

[18, 20] Jui-Cheng Yen and J. I. Guo showed that many encryption methods based on chaotic system. In this showed a new nonlinear chaotic algorithm (NCA) which used power function and tangent function place of linear function. In this algorithm in a one-time and one password system is used. J. Cheng; J.1. Guo proposed an image encryption algorithm is used it is based on a binary sequence generated from a chaotic system. It disorganized an image according to the generated binary sequence.

[4] Amitava Nag and Jyoti Prakash Singh proposed a method in which image encryption process is divided into two phase. In first phase shuffling the image pixel by affine transformation it relocates image pixels and second using XOR operation on image.

Compression is the process to reduce the data. Compression reduces number of bits.

[9] Dipti Kapoor Sarmah and Neha Bajpai showed Compression is the process that reduces size of data. Compression makes storing easier for large amount of data.

Compression technique can be lossless and lossy. There are many lossless compression techniques proposed some of main techniques such as Huffman coding, Run length encoding, Arithmetic encoding and Dictionary based encoding.

[8] Mamta Sharma and S.L. Bawa showed Huffman coding is a lossless data compression technique. Huffman coding is based on the frequency of occurrence of a data item is calculated. It is simple, and high speed by these properties Huffman coding is used.

### 3. SUGGESTED METHOD

In this paper, we suggested a method to get higher security for the data that embedding inside cover image without visible alternation in cover image. In suggested method has three phases of data security compression, encryption, and steganography.

1. Compression
2. Shuffling(Encryption)
3. Substitution (Steganography)
4. Reshuffling (Decryption)

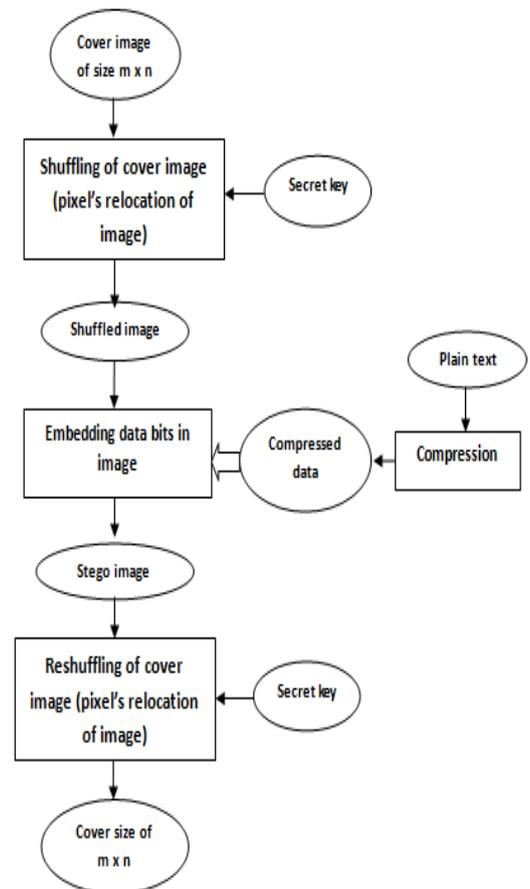


Figure 4. Data hiding in image

**Steps:** In compression reduces input text. In Encryption state cover image encrypted by changes location of pixel.

Insert compressed data into shuffled image. Image reshuffled in original form it containing secret data.

#### 4. APPLICATION

1. It is useful for vital information storing and confidential communication. It is valuable for intelligence agencies throughout world to exchange confidential information.

2. Mobile communication uses various mode of steganography for secure communication such as SMS and MMS based steganography. SMS and MMS are text and image steganography are used.

3. Steganography is used in Medical fields as a medical imaging system where a confidentiality between patient and physician.

#### 5. CONCLUSION

In this paper compression, encryption and steganography is suggested. First compression reduces actual size of data that increase volume of data. It can increase secret message bit in image. Affine transformation is used for scrambling operation that break correlation of neighboring pixels make image unidentifiable. A Steganography method is used this based on fuzzy pixel value differencing and modified LSB substitution.

#### REFERENCES

- [1] Masume Sabokdast, Majid Mohammadi, "A fuzzy approach for data hiding in images" *Fuzzy Systems (IFSC), 2013 13<sup>th</sup> Iranian conference on 27- 29 Aug. 2013*, pp. 1-6
- [2] A. Ioannidou, S. T. Halkidis, and G. Stephanides, "A Novel technique for image steganography based on high payload method and edge detection," *Expert System with Applications*, vol. 39, pp. 11517-11524, 2012.
- [3] Anil Khurana, B. Mohit Mehta "Comparison of LSB and MSB based Image Steganography" ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print) *IJCST* Vol. 3, Issue 3, July - Sept 2012
- [4] Amitava Nag, Jyoti Prakash Singh "Image Encryption Using Affine Transform and XOR Operation" *proceedings of 2011 International Conference on signal processing, Communication, Computing and networking Technologies 2011*.
- [5] C. H. Yang, C. Y. Weng, H. K. Tso, and S. j. Wang, "A data Hiding scheme using the varieties of pixel-value differencing in multimedia," *The journal of system and software* vol. 84, pp. 669-678, 2011.
- [6] X. Liao, Q. Y. Wen, and J. Zhang, "The steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image R*, vol. 33, pp. 1-8, 2011.
- [7] T. J. Ross, *fuzzy logic with engineering applications*, vol. 3. Wiley, 2010, pp. 1-160
- [8] Mamta Sharma, S.L. Bawa, D.A.V. college: "Compression Using Huffman Coding", *IJCSNS International Journal of Computer science and Network Security*, VOL.10 no.5, May 2010
- [9] Dipti Kapoor Sarmah, Neha Bajpai "A new horizon in Data security by Cryptography & Steganography" (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, Vol. 1 (4), 2010, 212-220
- [10] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *The journal of system and software*, vol. 81, pp. 150-158, Apr.2008.
- [11] C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," *IEEE Trans. Information forensics and security*, vol. 3, pp. 1556-6013, 2008.
- [12] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and replacement LSB methods" *Pro. Inst. Elect. Eng., Vis. Image Signal process.* vol. 152, pp. 611-615, 2005.
- [13] C. C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognition Letters*, vol. 25, pp.1431-1437, Apr. 2004
- [14] W. Stallings, *Cryptography and Network Security principles and practices*, 3rd ed., Pearson Education, 2003.
- [15] D. C. Wu and W. H. Tsai, "A steganographic method for images By pixel-value differencing" *Pattern recognition Letters*, vol. 24, pp. 1613-1626, 2003.
- [16] M. V. Droogenbroeck, R. Benedett, "Techniques for a selective Encryption of uncompressed and compressed images," in *proceeding of Advanced Concepts for Intelligent Vision Systems*, 2002, pp 9-11.
- [17] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", *Pattern Recognition and Image Analysis*, vol.10, no.2, pp.236-247, 2000.
- [18] J. Cheng; J.1. Guo, "A new chaotic key-based design for image encryption and decryption," *The 2000 IEEE International symposium on Circuits and systems volA*, no. 4, pp. 49 - 52, May.2000.
- [19] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - A survey," *Proceedings of the IEEE*, vol 87 pp. 1062-1078, 1999.
- [20] Jui-Cheng Yen and J. I. Guo, "A New Chaotic Image Encryption Algorithm," *Proc. 1998 National Symposium on telecommunications*, pp.358-362, Dec, 1998.

- [21] S. Walton, "Image authentication for aslippery new age," Dr.Dobb's journal, pp. 18-26, Apr. 1995
- [22] L. F. Turner, "Digital data security system," Patent IPN WO 89/08915,1989.