Exploring Digital Image and Video Steganography

Manveer Kaur Garcha
Department of Information Technology,
Chandigarh Engineering College
Landran, India

Jaskiran Kaur, Harsimran Kaur
Department of Computer Science
Chandigarh Engineering College,
Landran, India

***Abstract*—In this era of digitally driven world, it is imperative to secure digital information while communicating across the internet. Steganography is one of the techniques used for this purpose. This paper unfolds the need of steganography and the various forms of steganography. Also, it shed light on the general model of digital steganography with the terminology. The traditional method least significant bit substitution of steganography is discussed. Furthermore, a comparison is made between the traditional technique and one another techniques for quality of cover media and imperceptibility in terms of different performance metrics. Estimation about the size of secret message is made that can be embedded in the image.**

Keywords—Steganography; Embedding; Extraction; LSB

I. INTRODUCTION

In this digitally driven world of technology, nothing is assumed to be impossible. Along with the developments in techniques of data security, corresponding advancements are made in the field of hacking as well. So, the need of improving data security methods is increasing day by day. Steganography is one of the techniques for securing confidential information across the internet. The word steganography comes from Greek origin which consists of two words, namely, *steganos* and *graphie*. The word steganos means something that is protected and the word graphie means writing [1]. So, on the whole the meaning of term can be evaluated to be concealed writing. In other words, it can be explained as a secret communication technique in which only the sender and the recipient know about the existence of message [2].

Steganography went through many forms till date. Earlier, the Greeks used to shave the heads of their slaves and write message there. When the hair grew back, they send the slaves to recipients who again shave the heads to read the secret message. This method was really time consuming and offered limited space for writing the message [3]. In another form, steganography was carried out through wax tablets. In this technique, people used to write message on wood and cover it by wax. Then these wax tablets were sent to the intended receiver where the wax was peeled off in order to read that message [4]. Null ciphers were later on used as steganography during First and Second World War by the Germans. Here the useful message was encapsulated in a meaningless message. For example the first alphabet of every word of sent message may be plucked out to reveal the actual message [5]. Later, invisible inks were also used during the American Revolution by revolutionaries. Paper with messages written using such kind of inks were exposed to fire in order to read that message [6]. Today is the era of digital steganography. Multimedia such as image, audio or video can be used to hide the secret message in form of text from hackers while transmitting it over the internet.

Figure 1 shows the basic model of steganography. Cover media is the media used to hide the secret message. On the sender side, secret message and cover media act as an input to the embedding process. Embedding process refers to the sequence of steps used to hide the message and its output is the steganographic object. Steganographic object must be indistinguishable from the cover object because imperceptibility is the first and foremost requirement of steganography. On the receiver side, steganographic objects acts as an input to the extraction process, where extraction process is exactly the reverse of embedding process used to pluck out secret message from the input as an output [7].

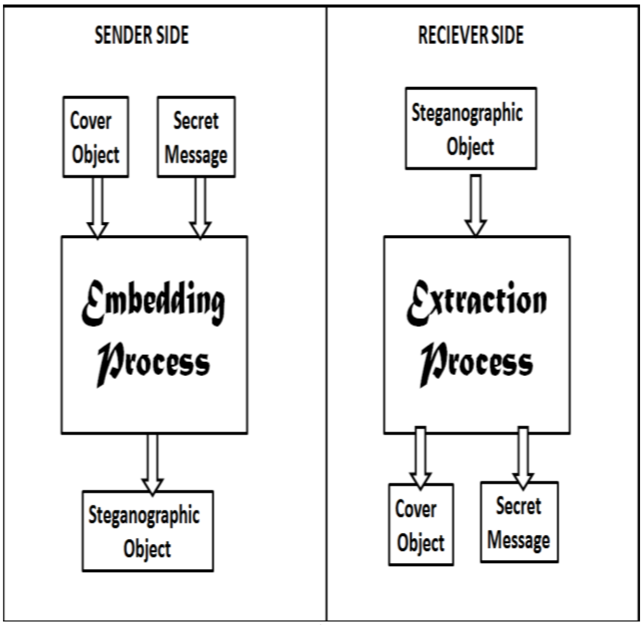

Fig. 1. Basic model of digital steganography

The rest of the paper is organized as follows. Section II describes the literature review. Section III gives a brief outline of various steganographic techniques followed by comparison of results in Section IV. Conclusions are drawn in Section V.

II. LITERATURE REVIEW

Anderson and Petitcolas (1998) defined steganography in detail and its scope that what can be done by steganography. Steganography is contrasted with related disciplines of cryptography and traffic security. A large number of approaches were outlined that were used to hide encrypted copy right marks or serial numbers in digital audio or video. Number of attacks was also presented on information hiding techniques [8]. Roque and Minguet (2008) proposed a novel technique based on the spatial domain: selected least significant bits. It worked with the least significant bits of one of the pixel color components in the image and changed them according to the message bits to hide. The rest of bits in the pixel color component selected were also changed in order to get the nearest color to the original one in the scale of colors. This new method was compared with other methods in spatial domain and the results were promising [9]. Khodaei and Faez (2010) proposed an image hiding method by using LSB substitution for improving stego image quality. In this method, secret message was transformed into a meaningless picture by using a bijective mapping function so that the difference of embedded secret message bits and LSB bits of host image pixels is of minimum possible value [10]. Mare et al. (2011a) introduced an optimization strategy based on the principles of genetic algorithms, that aimed to reuse the binary image color values in a controlled way so that instead of focusing to change the least significant portion of the color representation, secret data can be remapped in such a way that reduces the color information loss up to a negligible level [11]. Mare et al. (2011b) introduced a secret data communication system that employs the usage of two state-of the-art cryptographic algorithms (RSA with asymmetric keys and AES with symmetric keys) together with steganography. The joining of these three techniques built a robust steganography based communication system capable of withstanding multiple types of attacks, detection and reverse engineering [12]. Ananthi and Anjanadevi (2012) provided a reversible data hiding scheme that provides the ability to hide the data into a host image and then recover the host image without losing any information when the secret data is extracted. The proposed reversible image steganographic technique embeds secret message into error values of that image by using median edge detective predictor [13]. Sharma and Kumar (2013) proposed a steganographic algorithm based on least significant bit substitution to hide text file inside the digital image by using all the three layers of an RGB image alternatively to embed data. In order to increase the storage capacity, a compression algorithm was used that compresses the data to be embedded. Furthermore, two cover images were used. Message was embedded in the first cover image which was then covered by second cover image [14]. Moon and Raut (2013) used video frames as the cover image for hiding the message. Message is embedded using 1 LSB, 2LSB, 4LSB and 4LSB is found to be most suitable for hiding large chunks of information [15]. Kaur et al. (2014) introduced a hybrid standalone approach to steganography based on the least significant bit substitution. It aims to minimize the image degradation factor when message is embedded in cover image to form steganographic image by diminishing the data modification in least significant bits. In order to improve the security of message, the concept of jump table is used, i.e., message is scattered on the blocked image rather than embedding it on continuous pixels which makes extraction a semi-blind process [7].

III. STEGANOGRAPHIC TECHNIQUES

There are various techniques of digital image and video steganography. Video steganography can be seen as image steganography. In video steganography, the cover video is first divided into frames. Frames are still images extracted from that video. Then any of the frames is nominated to embed the message in it. After the embedding process is completed, the frame is again added into the video on its place. In comparison to image steganography, video steganography can be considered better as it is difficult to judge the presence of confidential information in moving frames.

A. *Least Significant Bit Substitution Method*

The least bit substitution method is considered as the traditional method of digital image and video steganography [15]. In order to understand how this technique works, consider an example as follows. Let the secret message to be hidden is '*Hello*'. Convert it into binary form.

01101000 01100101 01101100 01101100 01101111

Let the 1st, 2nd and 3rd pixel values of cover image to be **00001111, 10110010** and **01101101** respectively. Now in order to embed the first two message bits, i.e., 01 in first pixel as per LSB method, following changes are made to the two least significant bits of first pixel which are shown in Fig. 2.

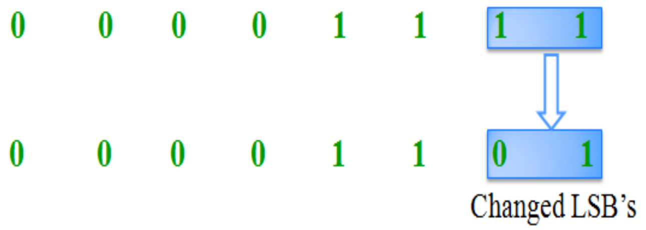

Fig. 2. Replacement of LSB's with message bits

Similarly, the LSB's of second pixel will remain unchanged from 10 to 10 as message bits are same, the LSB's of third pixel will change from 01 to 10 and so on until the whole message is embedded into the cover media, whether it is image or video frame.

B. *Video steganographic technique 1*

Video steganographic approach discussed in this section is proposed by Garcha et al [16]. This is an extension of LSB technique. In this method, frame is plucked out from the video logically on the basis of secret key. After the selection of frame, the two LSB's of pixel are changed with message bits. It is called as error factor 1. For an illustration, consider the pixel value to be 01101001 and the message bits to be 11. Then, EF1 is calculated by using following method. Primarily, the two LSB's of pixel are replaced with message bits and the value comes out to 01101011 as traditional LSB method. Then, LSB's of original pixel value are subtracted from the new pixel value to calculate EF1.

$$EF1= (11 – 01) = 01$$

Later, the LSBs of actual pixel are substituted with EF1. As earlier, the LSBs of actual pixel are subtracted from EF1 to calculate EF2 as shown below.

EF2= (01-01) = 00

It is understood that replacing the LSB's of original pixel with EF1will produce less error instead of changing the LSB's with message bits. If EF1 is greater, then LSB's are changed with EF1 and if EF2 is greater, pixel values are directly changed to message bits.

IV. DISCUSSIONS

The above mentioned techniques are compared for message size, security and quality. The quality is talked in terms of imperceptibility of secret message in cover media.

TABLE I. COMPARISON OF VIDEO STEGANOGRAPHIC TECHNIQUES

Performance factors	2 Least Significant Bit Method	Video Steganographic Method 1
Message Size	Equal	Equal
Security	Less	More
Imperceptibility	Less	More

For the evaluation of above table 1, first consider the message size. To find the message length that can be embedded in the image or frame, consider an image of size 512*512 pixels. Then,
Total number of pixels in image= 512×512=262,144;
Now, the number of bits that can be embedded in one pixel=2;
Number of bits in 262,144 pixels=262144/2=131,072;

If the character is of 1 byte, i.e., 8 bits
Then, 1 character can be embedded into 4 pixels
Number of characters in 262144 pixels= 262144/4=65,536;

If average number of words in character is considered to be 6
Then
One word can be embedded in 6×4=24 pixels
Then words that can be embedded in this image=262144/24=10,922 words.

The number of bits to be embedded in message depends on the number of least significant bits changed of an image. It can be 1 bpp (bit per pixel), 2 bpp, 4 bpp and so on. However, this may affect the quality of the over media. Changing more bits will obviously add more noise to the media.

Next factor is security of message. The security of message of simple LSB method is little less than the above mentioned technique. This is because the new technique used secret key which is required to find out the frame in which the confidential information is hidden. In traditional method nothing such is required.

Both the above factors, i.e., security and size are concerned with the message to be embedded, whereas the next factor quality is concerned with the cover media. If the quality of cover image will be less, the distortions will become visible. In this way, the hacker will get to know that there is something hidden inside and he may try to extract and read it. So, this is the most important thing to be considered while developing a steganographic approach. There are various performance metrics available to keep a check on the quality of cover image. The mainly used factors are mean square error (MSE), peak signal to noise ratio (PSNR), correlation coefficient (CC) and structural similarity index measure (SSIM).

Correlation is the method of image analyses, which determines the displacement of objects and evaluates the similarity between original and steganographic image. The value of correlation lies between 0 and 1, where 1 represents similar images [17]. Peak signal to noise ratio, on the other hand, is used to evaluate the difference between two images. The range of PSNR is from 1 to infinity. It is measured in dB (decibels) [7]. Structural similarity index measure is used to determine the structural changes in an image independent of attributes like luminance or contrast. Its value again lies between 0 and 1, where 1 is an ideal value [18].

V. CONCLUSIONS

This paper presented a crystal clear view of the term steganography. This is not a novel technique. It has its roots in history; however, it has changed its forms. Now is the age of digital steganography. The main focus of steganography is to preserve the confidential information from hackers. Least bit substitution method is considered to be the traditional and oldest method of digital image and video steganography. There are many extensions of this method, one of which is discussed in this paper. Also, a comparison is made which shows that extended algorithm is better than traditional one. The various factors to be considered while embedding the message are discussed along with the performance metrics such as PSNR, CC and SSIM.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy Magazine, vol. 1, 2003.

[2] C. Christian, "An information theoretic model for steganography," Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, vol. 1525, pp. 306-318, 1998.

[3] N. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," IEEE Journal, pp. 26-34, 1998.

[4] P. Wayner, (2002), "Disappearing cryptography- Information hiding: steganography and watermarking", San Fracisco, California, U.S.A.

[5] S. D. Dickman, "An overview of steganography," James Madison University Infosec Techreport, 2007.

[6] A. Kumar and K. Pooja, "Steganography- A data hiding technique," International Journal of Computer Applications, vol. 9, pp. 19-23, 2010.

[7] P. Kaur, H. Singh, A. Gupta and A. Girdhar, "An improved steganographic approach to diminish data modification for enhancing image quality," International Conference on Medical Imaging, m-Health and Emerging Communication Systems, pp. 329-333, 2014.

[8] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," IEEE Journal of Selected Areas in Communications, pp. 474-481,1998.

[9] J. J. Roque, J. Minguet, "SLSB: improving the steganographic algorithm LSB". V Congreso Iberoamericano de Seguridad Informática CIBSI'09. Montevideo, Uruguay, 2009.

[10] M. Khodaei and K. Faez, "Image hiding by using genetic algorithm and LSB substitution", Lecture notes in Computer Science Springer, vol. 6134, pp. 404-411, 2010.

[11] S.F. Mare, M. Vladutiu and L. Prodan, "Decreasing change impact using smart LSB pixel mapping and data rearrangement," 11th International Conference on Computer and Information Technology, pp.269-276, 2011(a).

[12] S.F. Mare, M. Vladutiu and L. Prodan, "Secret data communication system using steganography, AES and RSA," 17th International Symposium for Design and Technology in Electronic Packaging, pp. 339-344, 2011(b).

[13] S. Ananthi and A. Anjanadevi, "Reversible image hiding using predictive coding technique based on steganographic scheme", vol. 2, pp. 27-33, 2012.

[14] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography", IJARCSSE, vol. 3, 2013.

[15] S. K. Moon and R. D. Raut, "Analysis of secured video steganography using computer forensics technique for enhance data security," Second International Conference on Image Information Processing, pp. 660-665, 2013.

[16] M. K. Garcha, J. Kaur and H. Kaur, "An improved video steganographic approach to enhance the security of embedded message," International journal of Engineering Research and Technology, vol. 5, pp. 472-475, 2016.

[17] J. L. Rodgers and W. A. Nicewanders, "Thirteen ways to look at the correlation coefficient," The American Statistician, vol. 42, pp. 59-66, 19

[18] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity" IEEE transaction on image processing, vol. 13, pp. 600-612, 2004.