An Extensive Survey of Literature on Image Steganography Algorithm

Palak Chouriya[1], Prof. Khushboo Verma[2]

[1]*M.Tech. Scholar,* [2]*Research Guide*

Department of Computer Science and Engg, Bansal Institute of Science and Technology, Bhopal

Abstract- Recently, the information hiding techniques have become an important practice in a wide areas and applications, including digital audio, video, and pictures which are equipped dramatically with imperceptible marks that possibly contain a hidden copyright notice, and a serial number, or even have the ability to directly assist in keeping an illegal copying process. The term image alludes to a two-Dimensional (2-D) function of light intensity. A digital image is one that has been described both in spatial coordinates and brightness. The components of such an advanced picture are called picture components or pixels. Digital image processing is concerned essentially with extricating helpful data from pictures. In a perfect world, this is accomplished by computers, with practically zero human intercession. Image processing is any form of information processing for which both the input and output are images, such as photographs. Now days the data communication with the security and its authenticity has became one of the prominent factors in deciding the quality of data being sent and the quality of data communication. The new generation of computer and its innovation gives fantastic and different approaches to Steganography. With the movement of the computerized age, advanced steganography has turned out to be more reasonable and ground-breaking as information is the spirit of digital communication. This work briefs a broad review of literature on different image steganography approaches.

Keywords-Image Processing, Image Steganography, Least Significant Bit (LSB), IWT (Integer Wavelet Transform).

I. INTRODUCTION

The explosive and unprecedented growth in information communication technologies in the last one decade has brought about a shift in the way information and data is stored and retrieved. From homes to offices to the cyberspace, information is currently processed, stored, retrieved and transmitted electronically. Consequently the safety and security of information and data has become a fundamental issue of concern. Steganography, a technique used to conceal the presence of secret data in innocent looking containers like digital images and video files comes in handy particularly in open systems environments like the internet and other computer networks where secure links are not used and thus making information in transit vulnerable to interception and attacks. Steganography "is the art and science of writing hidden messages inside innocent looking containers such as digital files, in such a way that no one apart from the sender and intended recipient realizes the existence of a hidden message". The secret message is normally embedded in a cover medium known as a stego file in a way that totally conceals the existence of any form of communication. Besides hiding important data for safety and confidentiality, this technique can also be applied in copyright protection for digital media including audio, video and images.

Digital images are the most widely used cover files in the world of digital steganography. The reason for this is pretty obvious as there is hardly a PC in the world today that does not make use of one image or the other. An internet website is not complete without the use of an image or a company logo. When secret data is properly embedded in a digital image, the human visual system can hardly pick the difference between an original image and the one containing the hidden information.

A steganographic system involves two parties: the sender who embeds the secret message in the cover medium and the receiver who extracts the message from the cover. The sender takes the "host" object, which represents the cover-object, and embeds a secret binary message produce a stego-object that is perceptually identical to the cover. The stego-object is then communicated along a public channel to the receiver. At the receiver the stego-object is used to extract the secret binary message. The public channel may be monitored by an active warden whose goal is to detect the presence of any covert communication taking place. The key (k) is optional as it may be included in embedding process. The key is specific to the steganography algorithm which ensures that only recipient who knows the corresponding extraction key will be able to decode the message from a stego-image.

A steganographic system scenario is presented in figure 1.1. If a sender wants to send the secret message M to some recipient over the insecure communication line, the sender embeds secret-message (M) into cover-image (C) by some embedding method to produce stego-image (S). The key K (optional) may be used to find out the location in C to hide the message. Then the stego-image (S) is send to recipient. Upon receipt, the recipient uses extraction algorithm to retrieve M (extracted message).

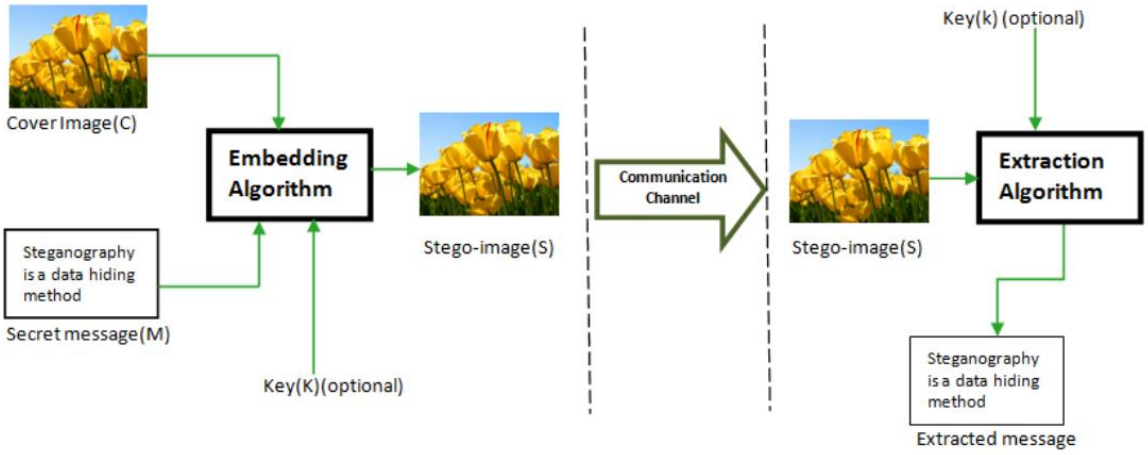

Fig. 1.1 Model of Image steganographic system.

II. LSB AND IWT TRANSFORM

The LSB approach is the most widely used steganographic algorithm to embed secret data into a carrier image. This technique embeds the bits of the secret message directly into the least significant bit plane of the cover-image following a deterministic sequence. The least significant bits of the carrier image are swapped with those of the secret information following a definite sequential pattern. Though this makes this approach perfectly imperceptible to the naked eye, its vulnerability to statistical steganalysis is relatively high.

In transform domain methods, the first step is to transform the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. These changed coefficients are transformed back into spatial domain to get stego image. The advantage of transform domain methods is the high ability to face signal processing operations. However, methods of this type are computationally complex. Steganography methods using Discrete Cosine Transforms (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transforms (DFT) come under this category [2]. In this work DWT and Integer Wavelet Transform (IWT) are used.

A. Least Significant Bits

Most steganography software hides information by replacing only the LSBs of an image with bits of the secrete file. This technique is generally called as LSB encoding. It is the easiest techniques used in steganography. The following example shows how the letter "A" can be hidden in the first eight bytes of three pixels in a 24-bit image. Example shows the eight pixels are updated with new values so on an average 50% changes are there at the bit position, because either the old bit would be replace by same value or by its complement value.

It is clearly shown that first bit plane that is Most Significant Bit (MSB) contains the useful data rather LSB plane. So one can replace only LSB to hide secrete data. When files are created there are usually some bytes in the file that aren't really needed, or at least aren't important. These areas of the file can be replaced with the information that is to be hide, without significantly altering the file or damaging it.

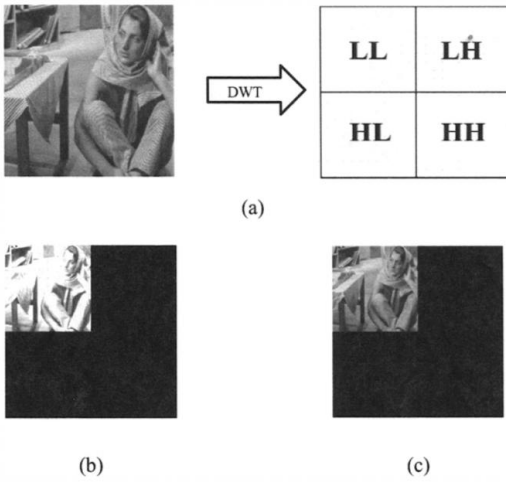

Fig. 2.1 Original image of Barbara and decomposed image using wavelet (b) One level of 2DDWT and (c) One level of 2DIWT decomposition.

This allows a person to hide information in the file and make sure that no human could detect the change in the file. The LSB method works best in picture files that have a high resolution and use many colors, and with audio files that have many different sounds and that are of a high bit rate. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted.

B. Integer Wavelet Transform

Since the discrete wavelet transform allows independent processing of the resulting components without significant

perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers the output can be completely characterized with integers. The LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted.

III. RELATED WORK

SR. NO.	TITLE	AUTHORS	YEAR	APPROACH
1	A secure image steganography algorithm based on least significant bit and integer wavelet transform	E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed	2018	Reported a secure steganography algorithm that hides a bitstream of the secret text into the least significant bits (LSBs) of the approximation coefficients of the integer wavelet transform (IWT)
2	Robust image hiding in audio based on integer wavelet transform and Chaotic maps hopping	S. E. El-Khamy, N. Korany and M. H. El-Sherif	2017	Reported a modified robust audio steganography technique that depends on integer lifting wavelet transform and logistic maps random sequence generation
3	High security data hiding using image cropping and LSB least significant bit steganography	K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby	2016	Reported a high security data hiding approach using image cropping and Least Significant Bit (LSB) steganography is reported
4	Efficient steganography using least significant bit and encryption technique	G. Sugandhi and C. P. Subha,	2016	Reported a new steganography approach for data hiding is reported by hiding data in the encrypted image using LSB (least significant bit) technique
5	High quality image steganography on integer Haar Wavelet Transform using modulus function	P. W. Adi, F. Z. Rahmanti and N. A. Abu,	2015	Reported approach which uses the modulus function on two adjacent coefficients to embed the message.
6	Performance improvement of IWT BPCS image Steganography	S. Sharma and U. Kumar	2015	Reported BPCS image steganography is a scheme with high payload capacity and it has higher invisibility against visual attacks
7	Real-time implementation of steganography in medical images using integer wavelet transform	S. Lavania, P. S. Matey and V. Thanikaiselvan	2014	Reported the real time application using the Integer Wavelength Transform (IWT) technique in the transform domain with the help of steganography.

E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed [1] The rapid development of data communication in modern era demands secure exchange of information. Steganog-raphy is an established method for hiding secret data from an unauthorized access into a cover object in such a way that it is invisible to human eyes. The cover object can be image, text, audio, or video. This work reported a secure steganography algorithm that hides a bitstream of the secret text into the least significant bits (LSBs) of the approximation coefficients of the integer wavelet transform (IWT) of grayscale images as well as each component of color images to form stego-images. The embedding and extracting phases of the reported steganography algorithms are performed using the

MATLAB software. Invisibility, payload capacity, and security in terms of peak signal to noise ratio (PSNR) and robustness are the key challenges to steganography. The statistical distortion between the cover images and the stego-images is measured by using the mean square error (MSE) and the PSNR, while the degree of closeness between them is evaluated using the normalized cross correlation (NCC). The experimental results show that, the reported algorithms can hide the secret text with a large payload capacity with a high level of security and a higher invisibility. Furthermore, the reported technique is computationally efficient and better results for both PSNR and NCC are achieved compared with the previous algorithms.

S. E. El-Khamy, N. Korany and M. H. El-Sherif,[2] Audio Steganography is the science of concealing any secret information in an unnoticeable cover audio file so as not to urge an eavesdropper's doubt. The target of this work is to present a modified robust audio steganography technique that depends on integer lifting wavelet transform and logistic maps random sequence generation. The robustness and security of hiding approach are increased with the encryption of the secret image by dividing it into blocks and the bits of each block are XORed with a different random sequence of logistic maps using hopping technique. The results show that this algorithm has acceptable levels of imperceptibility (indicated by peak signal to noise ratio (PSNR)) and good embedding capacity that can reach up to 25% from the cover audio file size. It also achieves full recovery of hidden data and robustness against attacks.

K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby, [3] A high security data hiding approach using image cropping and Least Significant Bit (LSB) steganography is reported. The predefined certain secret coordinate crops are extracted from the cover image. The secret text message is divided into parts with the same image crops. Each part of the secret text message is embedded into an image crop with secret sequence using LSB approach. The embedding is done using the cover image of three color channels. The stego image is given by reassembling the image and the stego crops. A detailed comparative study is performed between the reported approach and the other state-of-the-art approaches. This comparison is based on visualization to detect any degradation in stego image, difficulty of extracting the embedded data by any unauthorized viewer, Peak Signal-to-Noise Ratio (PSNR) of stego image, and the embedding algorithm CPU time. Experimental results shows that the reported approach is more secure compared with the other traditional approaches.

G. Sugandhi and C. P. Subha, [4] Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. A new steganography approach for data hiding is reported. In this approach hide data in the encrypted image using LSB (least significant bit) technique. The hidden data in the binary form is replaced to the LSB position of the encrypted image binary data. The hidden data will be recovered by the receiver using the secret key. Thus this method provides double staging security. Thus it will be used to reduce the chance of detecting the encrypted image and then provides advanced security level of the encrypted images.

P. W. Adi, F. Z. Rahmanti and N. A. Abu [5] A high demand on digital information in the last decade raises serious concern to protect its secrecy. Digital steganography hides the presence of a message in order to avoid an adversary attention. An image is the most popular medium of steganography. Hiding data into wavelet coefficients are able to maintain image quality. An Integer Haar Wavelet Transform (IHWT) is a method that transforms a 2D image into wavelet coefficients. IHWT which is derived from Discrete Wavelet Transform (DWT) can been suited to a human visual system (HVS). Moreover, IHWT coefficients are represented in finite precision which avoids the floating point problem of DWT. This work reported on improving the quality of stego image from the previous method that uses coefficient difference (CD) on IHWT. Instead of using CD that calculates the difference between coefficients, this work uses the modulus function on two adjacent coefficients to embed the message. The reported method has successfully reduced the effect on adjusted coefficients between two adjacent coefficients. This technique has led to an improvement on the stego image quality. The experimental results shows that the reported method achieved higher imperceptibility than the previous method.

S. Sharma and U. Kumar, [6] Steganography is the technique of embedding secret data into a cover medium which may be a video, audio or image. So it covers the presence of the hidden communication. BPCS image steganography is a scheme with high payload capacity and it has higher invisibility against visual attacks. Image steganography in frequency domain provides high robustness against statistical attacks. In transform domain Integer wavelet transform is much suitable as compare to DWT because IWT does not have to face fractional loss in transform coefficients. So IWT BPCS image Steganography is a better technique to improve payload capacity and robustness.

S. Lavania, P. S. Matey and V. Thanikaiselvan, [7] A method is presented to hide data within an medical image for the real time application using the Integer Wavelength Transform (IWT) technique in the transform domain with the help of steganography. IWT is an image compression

technique wherein the output is in the form of integers thus consuming less memory space. Steganography is done intelligently such that it is difficult for an adversary to detect the existence of a hidden message in the otherwise innocuous data. This united with integer wavelet transform allows high quality data hiding and image compression. To transmit many such images over a network, sometimes over low-capacity phone lines to remote sites, or to store large numbers of images over a long period of time as part of the medical records for patients, the need for image compression arises to alleviate these large demands for image data storage and transmission capacity. The secret information is hidden in cover image using IWT implementation which has been coded in C language to ensure easy realization in real-time applications. The PSNR and execution time for the different images using IWT technique have been computed.

IV. PROBLEM STATEMENT

Although the LSB method exploits the weakness of the human vision sensitivity (HVS) to hide secret data in a cover medium in such way that the human eye cannot perceive it, the statistical characteristics of the resultant stago images reveal high levels of distortion of the original cover images compromising on the security of the hidden data. Its hiding capacity is also relatively low as it uses only three bits in a single pixel or one bit per color channel.

To enhance and increase both the imperceptibility and the hiding capacity of the LSB method, this examination reviewed various recent approaches for image steganographic algorithms enhanced performance that makes use of varied number of bits per image color channel selectively picked across the entire image by use of the linear congruential random number generator. This is to help avoid the predictability of the places where the secret data is hidden in the carrier image thus enhancing imperceptibility by reducing the gap between the statistical characteristics of the original cover image and those of the stego image. The number of bits used per color channel can also be varied to accommodate more data and thereby enhance the hiding capacity.

V. CONCLUSION

This examination reported a brief survey of literature and related work in the field of data hiding and image steganography. The concept of information hiding is ancient technique which is traced back to a thousand years ago. It is merely based on dimming messages content by a process called encryption, which is sometimes not practically effective. In many competitive cases, it is highly demanded to suppress the initial existence of a communication in order to avoid suspicion from adversaries. Today, the term steganography is utilized in both legal and illegal activities. For legal activity it can be used in critical situation such as in war telecommunications, in order to conceal both the message and its source utilize spread spectrum or meteor, scatter radio. For the industry market application, with the advent of digital communications and storage, one of the most important issues is copyright violence, so digital watermarking techniques are being developed to restrict the use of copyrighted data.

REFERENCES

[1] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, June 2018.

[2] S. E. El-Khamy, N. Korany and M. H. El-Sherif, "Robust image hiding in audio based on integer wavelet transform and Chaotic maps hopping," 2017 34th National Radio Science Conference (NRSC), Alexandria, 2017, pp. 205-212.

[3] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 2016, pp. 400-404.

[4] G. Sugandhi and C. P. Subha, "Efficient steganography using least significant bit and encryption technique," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-6.

[5] P. W. Adi, F. Z. Rahmanti and N. A. Abu, "High quality image steganography on integer Haar Wavelet Transform using modulus function," 2015 International Conference on Science in Information Technology (ICSITech), Yogyakarta, 2015, pp. 79-84.

[6] S. Sharma and U. Kumar, "Performance improvement of IWT BPCS image Steganography," 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, 2015, pp. 1-5.

[7] S. Lavania, P. S. Matey and V. Thanikaiselvan, "Real-time implementation of steganography in medical images using integer wavelet transform," 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-5.

[8] Kaur S, bansal S, Bansal R K. "Steganography and classification of image steganography techniques". Proc. of International Conference on Computing for Sustainable Global Development, 2014: 870 – 875.

[9] Thanikaiselvan v, Arulmozhivarman P. , "High security image steganography using iwt and graph theory". Proc. of International Conference on Signal and Image Processing Applications, 2013: 337 – 342.

[10] Hemalatha S, Renuka A, Acharya U D, et al. "A secure image steganography technique using integer wavelet transform". Proc. of World Congress on Information and Communication Technologies, 2012: 755 – 758.

[11] El safy r o, zayed h h, el dessouki A, "An adaptive steganographic technique based on integer wavelet transform" Proc. of International Conference on Networking and Media Convergence, 2009: 111 – 117.

[12] Prabakaran G, Bhavani R, "A modified secure digital image steganography based on discrete wavelet transform" Proc. of International Conference on Computing, Electronics and Electrical Technologies, 2012: 1096 – 1100.