Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhancing the Data Hiding Capacity of Kekre Algorithm Using the Lempel–Ziv–Welch Technique

Ankush Garg*
M.Tech. Scholar (CSE)
BRCM CET, Bahal, India

Basant sah
Asstt. Prof. in CSE Deptt.
BRCM CET, Bahal, India

Abstract: Steganography is an art and science of writing hidden message in such a manner that no one apart from the sender & intended recipient even realizes there is a hidden message. It is a technique of invisible communication which hides the existence of the message. If the cover object used is an image, the steganography is known as image steganography. In this paper, we have proposed a data hiding method using the data compression technique and image steganography. This method improves the data hiding capacity of image as compared to existing method. In this method we compress the data by applying Lempel-Ziv-Welch compression technique and applying Kekre algorithm to hide compress data in image.

Keywords: Digital Image steganography, Data Hiding, Peak Signal to Noise ratio, Mean Square Error, Data Compression, LZW.

1. Introduction

Internet is the most popular medium that exchange information between parties. Most important factor of information technology and communication is the security of information. One of the aspects of information security is information hiding. Generally Information security means protecting information from unauthorized access, disruption, modification or simply illegal use. The three basic principles of information security are:

Confidentiality: Confidentiality is required for preventing the leaking of information to unauthorized user.
Integrity: Integrity means protecting the data from the modification by any unauthorized third party.
Availability: For any information system to serve its purpose, the information must always be available when it is needed.

1.1 Information Hiding Techniques

Many information hiding techniques have been developed for preventing data from unauthorized access. Main techniques used for data hiding are:

- Cryptography
- Digital Watermarking
- Steganography

(I) Cryptography

Cryptography is the science of secret writing. Cryptography transforms the original message without changing its information. Important terms used in the cryptography are:
Plain text: Actual representation of data or original message.
Cipher text: Coding form of data
Encryption: Convert plaint text into cipher text.
Decryption: Convert cipher text into plain text.
Key: key is used in encryption and decryption of data

The general concept of Cryptography is shown in Figure 1

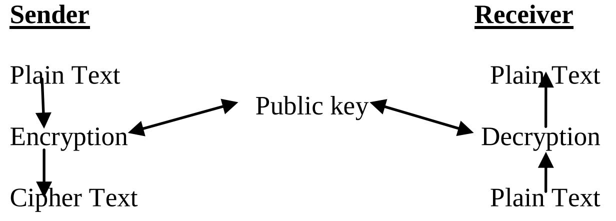

Figure 1: General Cryptography Concept

The typical scenario in cryptography is that sender wants to send some message secretly to the receiver. The message which is to be sent is in the ordinary language which is understood by all, i.e. the plaintext. The process of converting plaintext into a form which cannot be understood without having special information is called encryption. The unreadable form is known as cipher text and the special knowledge for encryption is known as encryption key. The conversion of cipher text again into plaintext with a special knowledge is known as decryption, whereas special knowledge for decryption is known as decryption key. Only the receiver has this special knowledge and only receiver can decrypt a cipher text with this knowledge called decryption key.

(II) Digital Watermarking

Digital watermarking [16] is the process of hiding the computer-aided information in a carrier signal. Digital watermarks can be used to verify the authenticity, integrity of the carrier signal. It can also be used to show the identity of its owners. It is mainly used for tracing copyright infringements and for authentication of banknote. Digital watermarks are perceptible under some conditions, i.e. after using some algorithm, and imperceptible anytime else if a digital watermark distorts carrier signal in a way that it gets perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be texts, audio, video, pictures, or 3D models.

Limitations of Digital Watermarking is that, someone interested in breaking the security mechanism imposed in watermarking can easily accomplish it by just replacing lines, replacing words or reshaping characters.

(III) Steganography

The word steganography comes from Greek word steganos which means covered or secret and the graphy means writing or drawing. So, literal meaning of steganography is “covered writing” [1]. Generally steganography is known as invisible communication. Cryptography provides confidentiality, steganography on the other hand hide the message and there is no knowledge of the existence of the message. In simple words, it is hiding the information into other information. Steganography and cryptography are different techniques. Steganography hides the information and cryptography protects the information. Due to hidden or invisible factor it is difficult to recover hide information. Procedure to know the steganography technique is known as steganalysis. In the basic steganographic process, the secret message is hidden into a cover object. The cover object can be any of text, image, audio, video etc. A secret key is also used and the secret message is embedded into the cover object using the secret key. This new message obtained is called stego message. The stego message is transmitted over the public channel. The receiver gets the message and retrieves the message using the stego key which is same as used by the sender. In this way security is achieved by hiding the existence of the message.

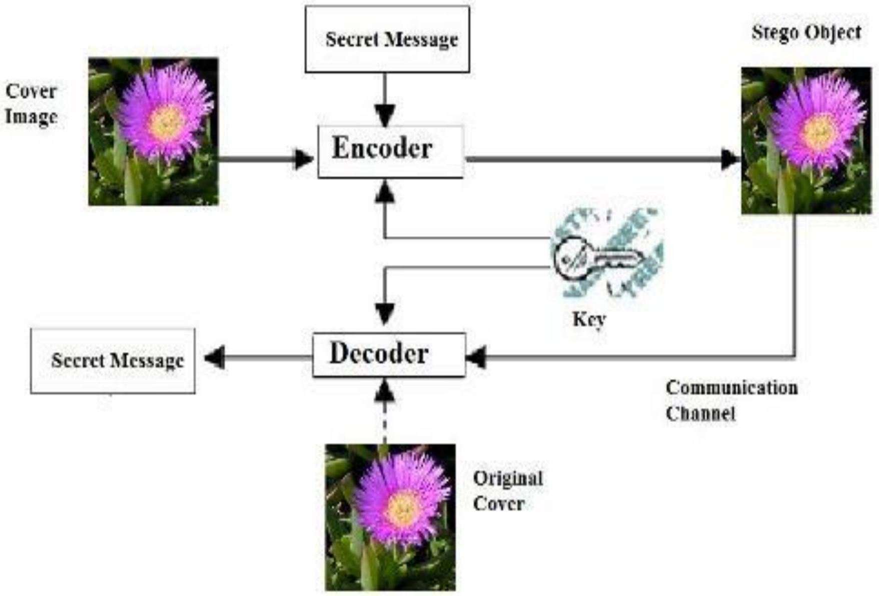

Fig 2: Basic Steganographic Process

Image steganography techniques can be divided into two groups:

- Image Domain also called spatial domain and
- Transform Domain also called frequency domain [5].

Spatial domain techniques embed information in the intensity of the original image pixels directly. Basically least significant bit (LSB) method is used where it replaces the least significant bit of original pixel with the message bit.

Transform domain also known as frequency domain where images are first transformed then the message is embedded in the image. *Discrete cosine transformation* (DCT) technique is used in JPEG images to achieve compression.

2. Related Work

Steganography is an area of invisible communication. It is not a modern technique which is used for protecting the unauthorized access of the information but is an ancient technique which is in existence since 440 B.C.

The most basic and important image Steganographic Technique is Least Significant Bit [4,8] embedding technique. In this technique data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this technique, least significant bit of each pixel is replaced with secret message bit until message end.But this technique has less embedding capacity and easy to detect.**Hamid et al. in [12]** discussed a texture based image steganography technique. This technique divides the texture areas into two groups. One is simple texture area and other is complex texture area. In Simple texture area 3 LSB bits of Red channel, 3 LSB bits of Green channel and 2 LSB bits of blue channels are used for embedding the secret data. In Complex texture area data is embedded into the 4 LSB bits of the pixel. This method increases the embedding capacity of the covered image.

Marvel [13] discusses spread spectrum image steganography technique. In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect. In spread spectrum image steganography the secret message is embedded in noise and then combined with the cover image which results into the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image. This technique provides high security than the previous techniques. However, this method does not provide sufficient data payload. ***Cheddad et al*.'s[15]** have proposed a region of interest (ROI) in image based adaptive steganography method. It selects required ROI in the image where it carefully hides the data bits. The selection of these regions is based on human skin tone color detection. Generally adaptive steganography methods are hard to target for attacks especially when the hidden message capacity is too small.

[6] *Yang et al*. proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image.

3. Proposed work

In the techniques discussed above, if the data embedded in the image is increased, the image quality deteriorates. So, we cannot embed sufficiently large data into the cover image. In our proposed technique we overcome this problem. We preprocess the secret data before embedding it into the image. The pre-processing reduces the size of the data by a significantly large amount which permits embedding the large amount of data into the same size cover image. Our proposed technique is based upon the intensity values of the pixels in the cover image. This technique can be applied to grey scale as well as color images. The preprocessed data is embedded into the cover image based upon the intensity values of the pixels in the cover image. For pre-processing, LZW(Lempel–Ziv–Welch) data compression technique is used. This method generates the stego image which is of very good quality.

In this technique sequence of 8-bit secret data is encoded as fixed-length 12-bit codes. The code from value 0 to 255 represents one character sequences consisting of the corresponding 8-bit character. As the data is encoded, the codes with values 256 through 4095 are created in a dictionary depending upon the sequences encountered in the data. A dictionary is initialized to contain the single-character strings corresponding to all the possible input characters. At every step in the compression process, input characters are gathered into a sequence until the next character comes that will make a sequence for which there is no code in the dictionary. The code for the sequence without the character encountered is emitted, and a new code for the sequence with the character encountered, is added in the dictionary. The algorithm works by scanning the input secret data for successively longer substrings until a string is found that is not in the dictionary. When such a string is found, the index for the string without the last character is fetched from the dictionary and sent to output, and the new string including the last encountered character is added to the dictionary with the next available code. The last input character is then used as the next starting point to scan for substrings. In this way, successively longer strings are added in the dictionary and made available for subsequent encoding as single output values.

In the decoding algorithm value is read from the encoded input and corresponding string is outputted from the initialized dictionary. The next value is read from the input secret data string, and adds to the dictionary the concatenation of the string just output and the first character of the string obtained by decoding the next input value. The decoder then proceeds to the next input value and repeats the process until there is no more input. The final input value is decoded without any more additions to the dictionary. The decoder builds up a dictionary which is similar to the dictionary used by the encoder. And this dictionary is used to decode subsequent input values. Full dictionary is not required to send to the receiver. The initial dictionary containing the single-character strings needs to be sent only. If the dictionary's initial values are decided beforehand by the sender and receiver, the initial dictionary too needn't be sent. This compression technique gives best results on the secret data with repeated patterns.

Steganography technique used is Modified Kekre Algorithm (MKA)[3,9]. In this technique, firstly 8-bit secret bit is selected. The secret bit is XORed with all the bytes of the secret message that is to be embedded into the cover image. For the pixels of the cover image having intensity value greater than 239; if the bit 1 is to be embedded then 5 bits of secret text are embedded and for embedding bit 0, 4 bits are embedded in LSBs of that pixel. For a pixel having intensity from 224 to 239; if bit to be embedded is 0, 5 bits of the secret message are embedded and for bit 1, 3 bits are embedded. For a pixel having intensity value in the range of 192 to 223, 2 bits are embedded otherwise only one bit is embedded. This method maintains a matrix of pixels whenever 5 bits of resultant secret message are embedded. The matrix also needs to be send to the receiver .This matrix helps in extracting the message from stego-image. By using the compression technique first and image steganography technique then, sufficient payload is achieved and without compromising with the quality of the image which is used to embed the secret data. Sufficiently large amount of data can be transferred in a more secure way by using our proposed technique.

4. Experimental Result

We carry out experiments by taking most widely used images and some other images for evaluating their performances and compared them with some existing techniques. The image quality metrics used are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Root Mean Square Error (RMSE). High PSNR value and low MSE value signifies good quality image. PSNR is measured in decibel (db). The images taken in our experiments include Chrysanthemum, Koala, Lighthouse, Penguins, and Tulips each of different dimensions. The secret data taken in our experiments is Abraham Lincoln’s letter to his son’s teacher that is embedded into each of these images which is of size 1785 bytes. The resultant stego images with hidden secret message, employing our proposed method are shown in Figures below.

The performance results are shown in Table 1.1, 1.2, and 1.3.

Table 1.1: PSNR values of Different Approaches on different Images.

Cover Image	Modified Kekre Algorithm	Proposed Algorithm
Chrysanthemum.jpg	67.1833	69.9992
Koala.jpg	67.3960	70.1354
Lighthouse.jpg	69.6649	72.7051
Penguins.jpg	71.8620	74.5735
Tulips.jpg	70.8246	73.6841

Table 1.2 MSE values of Different Approaches on different Images.

Cover Image	Modified Kekre Algorithm	Proposed Algorithm
Chrysanthemum.jpg	0.0124	0.0065
Koala.jpg	0.0118	0.0063
Lighthouse.jpg	0.0070	0.0035
Penguins.jpg	0.0042	0.0023
Tulips.jpg	0.0054	0.0028

Table 1.3 RMSE values of Different Approaches on different Images.

Cover Image	Modified Kekre Algorithm	Proposed Algorithm
Chrysanthemum.jpg	0.1115	0.0806
Koala.jpg	0.1088	0.0794
Lighthouse.jpg	0.0838	0.0591
Penguins.jpg	0.0651	0.0476
Tulips.jpg	0.0733	0.0528

It is evident from the above tables that the proposed technique is better than the existing technique and produces better results. For every image the value of PSNR, MSE and RMSE value of our proposed technique is better than the MKA technique [3].

(a) Chrysanthemum (b) Chrysanthemum

Fig 3 Chrysanthemum (a) Cover image and (b) Stego image

(a) Koala (b) Koala

Fig 4 Koala (a) Cover image and (b) Stego image

(a) Lighthouse (b) Lighthouse

Fig 5 Lighthouse (a) Cover image and (b) Stego image

(a) Penguins (b) Penguins

Fig 6 Penguins (a) Cover image and (b) Stego image

(a) Tulips

(b) Tulips

Fig 7 Tulips (a) Cover image and (b) Stego image

5. Conclusion and Future scope of work

In this work we explored the existing image steganography techniques. We proposed an efficient image steganography technique. In image steganography, image is used as a carrier for transmission of the secret information or data. The image used can be either gray scale or color image. In this technique data is firstly preprocess. This preprocessing reduces the size of the data by a significantly great amount. This preprocessed data is then embedded into the LSBs of the pixels of the image depending upon the intensity of the pixel values. Our proposed algorithm is targeted to achieve very high image embedding capacity into the cover image and more security of the secret data. The proposed technique performs better than MKA [3]. It has high PSNR value and low MSE value as compared to MKA. This preprocessing reduces the size of the secret data by a significant amount and thus permits more data into the same image. The embedding capacity of the proposed technique is very high as compared to MKA.

The work can be extended to provide an alternative strategy for data compression which can further reduce the size of the data. Efficient cryptographic techniques can also be used along with the steganographic techniques to provide more security to the data.

References

[1] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[2] N. Tiwari and M. Shandilya, “Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth”, International Journal of Security and Its Applications Vol. 4(4), Oct. 2010.

[3] H. B. Kekre, A. Athawale, P. N. Halarnkar, “Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Information Hiding in Images”, International Conference on Advances in Computing, Communication and Control, 2009 pp 342-346

[4] Deshpande Neeta, Kamalapur Snehal, ”Implementation of LSB Steganography and Its Evaluation for Various Bits” K.K.Wagh Institute of Engineering Education & Research, Nashik India

[5] Morkel, T., Eloff, J.H.P & Olivier, M.S., "An overview of Image Steganography", Proceedings of the Information Security South Africa (ISSA) Conference, 2005.

[6] H. Yang, X. Sun, G. Sun. “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”. Journal: Radio engineering Year: vol. 18, 4 Pages/record No.: 509-516, 2009.

[7] H.C. Wu, N.I Wu, C.S. Tsai and M.S. Hwang, “Image Steganographic scheme based on pixel-value differencing and LSB replacement methods”, VISP(152), No. 5, October 2005

[8] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Member, IEEE, and Hung-Min Sun, “Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems”, IEEE Transactions on Information Forensics and Security, vol. 3, no. pp. 488-497. 3rd September 2008.

[9] H. B. Kekre, Archana Athawale, Pallavi N. Halarnkar, “Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Information Hiding in 88 Images”, International Conference on Advances in Computing, Communication and Control, pp 342-346, 2009.

[10] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, “A high quality steganographic method with pixel-value differencing and modulus function”. Journal of Systems and Software, vol. 81, no. 1, p. 150-158, 2008,

[11] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo. ”Image data hiding method based on multi-pixel differencing and LSB substitution methods”. In Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08). Daejeon (Korea), Aug. 28-30, p. 355-358, 2008.

[12] Hamid, A. M., M. L. M. Kiah, et al. (2009). "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis" Internationa Journal of Engineering and Technology (IJET).

[13] L.M. Marvel “Spread Spectrum Image Steganography,” IEEE transactions on image processing, vol. 8, no. 8, pp. 1075-1083, August 1999.

[14] M. Hussain, M. Hussain., “Pixel Intensity Based High Capacity Data Embedding Method”, Information and Emerging Technologies, International conference 978-1-4244-8003 June 2010

[15] A. Cheddad, J. Condell, K. Curran and P. McKevitt, “Enhancing Steganography in digital images”, IEEE - 2008 Canadian conference on computer and Robot vision, pp.326-332, 2008.

[16] P.C. Gupta and M. Sharma "A Comparative Study of Steganography and watermarking", International Journal of Research in IT & Management (IJRIM), vol 2,issue 2, 2012.

[17] M.K. Kaleem "An Overview of various form of Linguistic Steganography and their applications in protecting data", Journal of Global Research in Computer Science(JGRCS), vol 3, no.5, 2012

[18] Gowtham Prasad T V S, Dr. S Varadarajan,"Image steganography Based on Optimal LSB Pixel adjustment Method", International Journal of Computer and Technology, vol 5, no. 1, 2013