International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 4 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT19548

Hiding Secret Data Using Image Steganography

Paridhi Tutlani[1], Mrs. Priyanka[2]
[1]M. Tech Scholar, CSE, I.G.U Rewari, SCET Mahendergarh, Haryana, India
[2]Assistant Professor, CSE, I.G.U Rewari, SCET Mahendergarh, Haryana, India

ABSTRACT

Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So, the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Hiding Secret Data Using Image Steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as image file. In this paper we mainly discuss different types of image steganographic methods, advantages and disadvantages.

We focus in this paper on Hiding Secret Data Using Image Steganography, which has emerged as a prominent source of data hiding across novel telecommunication technologies such as covered voice-over-IP, audio conferencing, etc. The multitude of steganographic criteria has led to a great diversity in these system design techniques. In this paper, we review current digital image steganographic techniques and we evaluate their performance based on robustness, security and hiding capacity indicators. The primary goal of steganography is to reliably send hidden information secretly, not merely to obscure its presence. Steganography in today's computer era is considered a sub-discipline of data communication security domain. Lately, new directions based on steganographic approaches started to emerge to ensure data secrecy. Rather than as a substitute to existing solutions, these approaches could achieve better data secrecy if combined with conventional security techniques. Modern techniques of steganography exploit the characteristics of digital media by utilizing them as carriers (covers) to hold hidden information.

Keywords : Steganography, Cryptography, Hiding Secret Data Using Image Steganography, LSB.

I. INTRODUCTION

By cryptography, the message structure is cracked down to make defective and unclear unless the advertising key is available. It does not make an attempt to hide or hide the message that is encrypted. In particular, cryptography provides the ability to transmit information to people in a way that prevents a third person from learning. Cryptography can also confirm the verification of someone or something In the steganography does not change the structure of the following points can be viewed in the steganography update.

The steganography app covers different types of data within the cover file. The leading stego also contains hidden information, although it is similar to a covered file. What the Steganography says in the use of human intelligence; human experience is not trained to search for hidden information inside it,

CSEIT119548 | Received : 20 June 2019 | Accepted : 14 July 2019 | July-August -2019 [5 (4) : 65-70]

although there are available programs that can do so called Steganalysis (Recognition of Steganography).

Information security is one of the most important features of information technology and communication as a result of the enormous growth of the World Wide Web and copyright laws. Cryptography was developed as a way of obtaining confidential information. Unfortunately, it is sometimes not enough to keep the details of the message confidential, so it may be necessary to keep the secret of the message and the idea behind it called steganography. Steganography is a habit of hiding a secret message from any media. Most details of secrecy use the advantage of personal weaknesses. The steganography is often confused by cryptography because the two are similar to the two used to protect confidential information. If both techniques: cryptography and steganography are used for communication with double protection. The main difference between Steganography and cryptography is that, screaming focus on keeping the content of the message while steganography focuses on making a private message. Steganography and cryptography are both required to protect messages from a third party but each has your own. Therefore, if necessary to protect the presence of the message; steganography is the solution [20]. Perhaps the most common cover sources are a combination of images, sound, and video. Here, on this page, we focus on pictures as sources of news. Two other technologies related to the steganography are watermarking and fingerprinting. These technologies have a profound effect on the protection of intellectual property. Examples of ordinary steganography requests are in the copyright protection field. According to [, the information hidden in the stream allows the video revival to resume. The only payout that should pay for a small amount of non-formal video quality, with a limited amount of computational design. Steganographic process receives its major request in the private sector. It can be used by intelligence agencies around the world to convert more confidential data to privacy sources, e.g. A secret agent can hide a map of a terrorist campus in a photo using steganographic imagery software and send it to a forum. An official from the head office can download a photo from the forum and easily find a hidden map.

II. PROPOSED SYSTEM AND METHOD

The proposed model is a powerful answer to finding safe information. It is defined by a specific goal of obtaining reliable information and isolation. Regardless of the information given on the system, there is no guarantee that information will be accessible on the basis of it.

The information hiding process consists of following:

Five modulus method:-

Modulus Method (FMM) was first proposed. The basic concept of FMM is based on the following concept: A common feature of photographs is that neighboring pixels are combined. Therefore, in the picture of the two letters, the peacock neighbors are often like a real pixel.

Proposed steganography algorithm

According to the previous section, the FMM transformation does not affect the Human Visual System (HVS). The proposed algorithm was called ST-FMM which means STeganography by the Five Modulus Method. Therefore, all the pixels inside the FMM images are all multiples of 5 only. Hence, the values that are not divisible by 5 are distinct inside k block. Obviously, it is known that the standard ASCII×k code consists of 128 characters.

Determination of Window Size

The ideal size of the window used for steganography is a very important way. Small style size is better to increase the number of hidden messages in the cover photo.

Watermarking for providing the copyright or ownerships for that image

Includes an undetectable watermark is a common way to see images and protect them from unauthorized use on the web. Watermark is a visual feature installed on computer software containing content, symbol, or copyright notification. The reason for watermark is to recognize the activity and limit its use. In spite of the incomprehensible watermark cannot prevent unauthorized use, it makes it even more difficult for people who may need to call someone else's photo or art work like them. It should be considered that ensuring that the watermark is enforced, not only to prove that the image has been changed, and in addition to teaching individual individuals about copyright and inheritance. Ideally, watermark must be a copyright image next to the owner's name, and the owner's site URL, if appropriate. This goes beyond the copyright message, and gives others the opportunity to contact the original image owner. Watermark status can be a manageable function. Watermark must be deliberately designed to remove the image, but instead you can choose not to put a watermark in the Shading region of a solid or a fixed distance where the dismissal may be but it is difficult to cover. In the case of watermark security, hold small amounts of light in the light.

III. RESULTS AND DISCUSSION

Embedding a picture watermark

Here is the full code of the DrawImage (Image) system, which makes all control of the image, and later will show the code for other details. Before we really look at the watermark in the photo, we have to love a watermark photo, check the limits and measurement settings. Personal process GetWatermarkPhotos (Photo) returns the original watermark image when the monitoring and kick settings are default; often, another bitmap is made by new sizes, including edges and measurements with the same degree of determination like the first watermark image. The first watermark image is drawn to the latest bitmap yet. Next, the watermark indicators are calculated on the GetWatermarkPosition independent plan, which works well with the image of the watermark image, so the image is currently in new edges and accumulates. If we analyze the image guidelines before we change them (that is, changes that affect the size of photos), we will not clearly understand the directions. At the moment, we are said to use the injustice and we specifically develop our image of the watermark.

The Hiding Technique for Hiding the Data Into The Image

The proposed program has the following categories: uses a private key and a weighting frame to verify the hidden information, using a weighting network to create hidden information in value and uses the XOR administrator to increase security. Moving information is usually performed by changing the wrong data from the event message. For example, you are given a picture of a shading, a small clip (LSB) for all pixels can be changed to insert a black mystery. An encrypted program because of the frequency of broadcasting the radio is proposed. The focus on security records (e.g., fees) is mentioned. Individuals use cryptography encryption to send private messages outside of someone else's message. The steganography type of cryptography where a secret message is included in a computer image. Think of each of those pixels in the picture and the whole pixel has three shading numbers - there are zillions in the picture. If the customer has changed a few numbers of these shading figure the next image will look much like the original image; Indeed, most could not tell that the client changed the image in any way. Steganography works by changing a number of pixel shading; The client will use special pixel attributes to talk to characters rather than shading. Of course, the next picture will look as much as the first ones without the fact that the "blips" of the little ones may seem insignificant if the client looks carefully. The client can send a photo to a partner and can delete the message at a time when it can be detected by pixels.

The client can send a photo to a partner and can delete the message at a time when it can be detected by pixels. Starting with a client you should read a photo as a jpg and then set aside 24-bit bmp in a group or simply keep a photograph of the design bmp customers should use the bmp record of this activity unless the jpg "is lost" means which buyer continues interacting with a document can be changed in some way so that the next image can be removed more freely. In this way jpg won't work for steganography because jpgs will change the privacy message when deleting the document to install it. Here are your records keeping. You can give it the same name without making sure you have entered the recordings of the .bmp at the end. (For example, a user uploaded "Matt.jpg" and saved "Matt.bmp"). Writing / stopping method

- ✓ The user can distinguish your picture pixels into one major category using a text to get Pixels() strategy.
- ✓ Use the main pixel (in 0 place) to cover the length of your message (number of characters). The buyer will block existing messages from around 0 and 255 characters long.
- ✓ After this use each eleven pixel to cover the letters in your message. Start with pixel 11, then pixel 22, thus until the client celebrates all the characters in your message.
- ✓ The thing that the client needs to cover in pixel is 8-bits in length. Length (in main pixel) byte. The buyer can convert all bytes and bytes.
- ✓ Use this process to hide all favorites in a suitable pixel.

Two Steps

a. Identification of redundant bits in a cover-file. Redundant bits are those bits that can he modified without corrupting the quality or destroying the integrity of the cover-file.
b. To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

Hiding Secret Data Using Image Steganography Methods

Lsb Coding
Hase Coding
Spread Spectrum
Echo Hiding

IV.CONCLUSION

From the above-mentioned algorithm suggests a new steganographic algorithm. In this information they are photographed and sent onto the system where its recognition is checked and a hash-based measurement test or photo. The proposed work provides secure securities between the sender and the collection, ensuring that the information entered is always orderly and non-refundable, watermarks the image with a visible visible quality without bringing significant losses. It is useful in making copyright material declaration. Compiled information cannot be successfully extracted and contradicted common image control techniques.

V. FUTURE WORK

- ✓ Use an algorithm to create a watermark in a 3D image, and more and make copyright to them so that there are no body parts in your audio and other video.

- ✓ Try to create an algorithm to include audio and video information for the client can send audio or video marked notes and the recipient can be able to do without much easier recover information.

VI. REFERENCES

[1]. W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Data Hints", IBM Systems Journal, Volume 39, Issue 3-4, July 2000, p. 547 - 568.

[2]. Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly Swarnendu Mukherjee, "Steganography Teaching Tutorial", International Conference Contemporary Computing (IC3-2008), Noida, India, August 7, 2008, p. 105-114.

[3]. Robert Krenn, "Steganography and Steganalysis", Article, January 2004.

[4]. Nedeljko Cvejic, Tapio Seppben "Increasing LSB capacity based on concealing confidential data using Steganography image" FIN90014 University of Oulu, Finland, 2002.

[5]. Sajad Shirali-Shahreza M.T. Manzuri-Shalmani "A high-level communication error on a domain's wavelet domain steganography "ICASSP 2008

[6]. Neil F.Johnson, Z.Duric and S.Jajodia. "Steganography hiding and Watermarking attacks." and monitoring ", the Kluwer Academic Publishers, in 2001

[7]. F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn: "Hiding Information-Testing", The IEEE process, vol.87, no.7, p. 1062-1078, in July, 1999.

[8]. Min Wu, Bede Liu. "Multimedia Data Hiding", New Springer-Verlag in New York, in 2003.

[9]. N. Port-Delgarm, "Watermarking Talk", MSS. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006.

[10]. M. Pooyan, A. Delforouzi, "LSB encrypted data by using the Steganography image A method based on the raising of Wavelet Convert ", Proc. Ith IEEE International International Symposium for Processing Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[11]. R. A. Santosa and P. Them, "wave-to-image conversion-based conversion based on Hide Data Data Using the Image Steganography," Mc. of 47 Int. Symposium ELMAR, June 2005, p. 209- 212.

[12]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "Real-Time Steganography Based on Audio-to-Audio Data Bit Stream ", IEICE, ISEC, vol.106 pp.15-22, September 2006.

[13]. Aoki, Naofumi. "VoIP Network Connection Process Using Steganography Technology", IEICE, SP, 106 (333), pp.31-36, 2006.

[14]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe International Conference on Intelligent "Hiding Information and Multimedia Isign Processing Processing" © 2008 IEEE.

[15]. A. Delforouz, Mohammad Pooyan, "Adaptive Digital Hiding Data Hidden Data Using Steganography Image Based on waveglegraphic integer modify ", IEEE Third Conference of the World of Work Secret Information & Multimedia Spot Analysis, 2007, 26-28 Nov 2007, p 283-286.

[16]. R. A. Santosa, P. Bao, "Conversion of the Transform Audio-to-Image based on a hidden image by using a Steganography image", 47th International Symposium ELMAR-2005, 08-10 June 2005, Zadar, Croatia, pp 209-212.

[17]. S. Shirali-Shahreza, Mr. T. Manzuri-Shalmani, "Transformed Wavelet Domain to Hide Password Data Using Image Steganography

Capacity High and Error Low Rate ", the IEEE International Conference on Information and Emerging Technology, 2007, 06-07 July 2007 p 1-5.

[18]. Yincheng Qi, Jianwen Fu, and Jinsha Yuan, "Wavelet of the steganalysis base based database" histogram times, "Journal of System Simulation, Vol. 20, No. 7, p. 1912-1914, April 2008.

[19]. Yin-cheng qi, liang ye, chong liu "stevealysis of Wavelet domain audio repetition model "International Conference of 2009 Conference on Analysis Wavelet and the Prophet Recognition, Analysis, 12-15 July 2009.

[20]. V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.

[21]. Mengyu Qiao, Andrew H. Sung, Qingzhong Liu "Feature Mining and Intelligent Computing for MP3 Steganalysis "The United Nations Summit on Bioinformatics, Systems Biology and Intelligent Computer 2009.

Cite this article as :

Paridhi Tutlani, Mrs. Priyanka, "Hiding Secret Data Using Image Steganography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 4, pp. 65-70, July-August 2019.

Available at doi :
https://doi.org/10.32628/CSEIT19548
Journal URL : http://ijsrcseit.com/CSEIT19548