IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Introduction to Image Steganography Techniques

Sonu Kumar
Lovely Professional University
Jalandhar Punjab

Akash Dilkumar
Lovely Professional University
Jalandhar Punjab

Priyanka Gupta
Lovely Professional University
Jalandhar Punjab

Twinkle Sharma
Lovely Professional University
Jalandhar Punjab

Abstract—Image steganography is a way to provide hidden data to a host image to transfer it safely. There are many ways to do this. Choosing the right algorithm is a necessary step. This paper introduces a study of the famous steganography techniques and discusses its beauty, limitations, and their comparative performance. The basics of steganography imagery, the features of steganography imagery are covered in paper. Image steganography techniques can be categorized according to different criteria. Separation is also included in this paper. Five main ways of photographs reported in this paper. An in-depth analysis of each method, their relevance, and the reduction and comparison of strategies are performed in this paper. Various stainless-steel tracks are also covered. With access to confidential information to be sent, security provision is an unavoidable issue that will not be compromised. The most widely used algorithm in this field has a huge gap. This is the state of cracking of hidden messages in an image file. This is due to the simplicity of the algorithm that provided a place for easy cracking of messages. Therefore, the Security Extensibility algorithms are called the SRM steganography algorithm. (Abstract)

Keywords—digital image; information hiding; multimedia security; watermarking; steganography

INTRODUCTION

The art of hidden information in digital media. Steganography and watermarking aim to embed private information on coverage for the purpose of identification, copyright protection, and annotation. Data encryption techniques fall into three categories of cryptography, steganography, and watermarking. Watermarking and especially steganography tend to hide the presence of data encryption while cryptography makes data gibberish.

Media representation in digital format facilitates its accessibility and improves accuracy, efficiency, and portability of data availability. But on the other hands the negative effects of the possibility of copyright infringement and modification or distortion of content. Intellectual property protection, content indexing, and annotation are the main reasons for promoting the use of these strategies.

Digital data encryption falls into various categories such as inserting copyrighted information into different digital media formats such as text, audio, image, or video with the effect of downgrading that may be visible on the host signal. For example, results should be invisible or invisible to its viewers. Data encryption techniques are different from encryption techniques as they aim to make embedded data inaccessible and illegal.

The amount of encrypted data and data intrusion fraud requires different methods of data embedding and there is no single method

it can access all the goals and then require various classes of strategies to extend the entire range of the application.

The main use of digital media encryption techniques retains copyright and ensures content integrity. To achieve the stated objectives embedded data must be kept encrypted in the host signal even if it is subject to degrading fraud such as lost data compression, cropping, sample retrieval, or filtering. Since embedded data and both the author and the consumer all data encryption details, such as additional data insertion, must be consistent in deletion or detection.

Image Steganography where data is hidden inside an image file. The selected image is called the cover image and the image obtained after the steganography process is called steganographic -image. Image steganography is of various types. In a photo booth the image is usually a holder that holds private information. In the diagram below, the cover image shows an image used to hide private data as a paid upload. Embedding process is a useful algorithm for hiding a secret message inside a cover image with the help of a steganographic key. The steganographic key needs to be shared on both sides. 'Steganographic-image' is the final release image that keeps private information hidden. There is also an extraction process used to get a private message from steganographic -image with the help of steganographic -key. The counter of steganography is steganography or steganography attacks. "steganography is the art and science of discovering the existence of secret messages or images.

BackGround

As the various papers and resources responded to the image steganography it had been important to grasp and understand on what basis they were built and divided. The steganographic method of the image is tested supported the subsequent particularly

• Embedding capacity - what's the most input load that may be achieved

• Visual image quality - How similar the steganographic image and canopy image are

• Security - How can a steganographic image protect itself from various steganography attacks?

A good steganographic method should complement the points mentioned above. But high steganographic payment methods expose things that are distorted in stage images and make them susceptible to steganography testing. Also, steganographic techniques with high visual image quality suffer from low pay-outs. Therefore, getting a high payload, high visibility quality, and non-availability at the identical time may be a challenge. Proposed steganographic methods will be classified in line with different criteria. Understanding segregation also will help us in understanding the ways. Distinguishing them supported the model process also can be categorized into differing types supported their functionality. are divided supported embedding domain, local domain and conversion domain. The flexible embedding method is additionally under the above category because it will be utilized in both local and conversion domains. this is often mainly supported their common goals or objectives. 2b shows a second kind of classification supported different steganographic techniques designed specifically to spot coded image formats, namely raw (BMP), compressed (JPEG2000) and encrypted image data (advanced AES encryption). 2c relies on segmentation supported steganographic techniques designed in relevancy the format / style of confidential data. This classification of steganographic techniques relies on various sorts of confidential data.

DIFFERENT STYLE OF IMAGES

User must run the appliance. The user has two-tab options – encrypt and decrypt. If user select encrypt, application give the screen to pick out image file, information file and choice to save the image file. If user select decrypt, application gives the screen to pick out only image file and ask path where user want to save lots of the secrete file.

A. Least Significant Bit Insertion

It is an image of the local background of steganography. Local domain embedding methods are generally more popular than the conversion domain because they are easier to embed with the extraction process. But they are often less powerful.

Inserting at least a Significant Bit (LSB) is a well-known steganography image algorithm. Includes LSB image layer modification. In this method, the message is saved in LSB pixels which can be considered as random sound. Therefore, changing them has no obvious effect on the image.

This method converts the last few bits by byte to insert a useful message especially in the image mode, where the red, green, and blue values of each pixel are represented by eight bits from 0 to 255 decimal or 00000000 to 11111111 now binary.

For example changing the last two pieces with a complete red pixel from 11111111 to 11111101 only changes the red value from 255 to 253, which when the human eye makes a change that is almost invisible to color but still allows us to encode the image inside.

This method works best for media files where small changes in byte values cause very small invisible changes. But that is not the case with the ASCII text where one thing that is out of place will completely change the character. Hidden information using LSB steganography is easy to find if you need it.

B. Redundant Pattern Encoding

Unwanted pattern repetition is the same type of spectrum distribution process. In this process the message is spread throughout the image, based on an algorithm. Therefore, the image based on this process cannot be cut or rotated. Many low-resolution images increase the chance of recovery, or in cases where a steganographic image is used.

In the event of an unwanted pattern insertion, a small message can be replicated repeatedly so that when the steganographic image is cut there is a greater chance that the watermark can still be read.

C. Encrypt and Scatter

This method hides the message as white noise. It is widely used in steganography. An example of it is the White Noise Storm which uses spectrum propagation and frequency hopping. The previous window size and data channel are used to create a random number. The message has spread to all eight channels in this random number. Each of these channels enters, circles and alternates with all other channels. One channel is less representative so there are more unaffected elements in each channel.

In this way it is very complicated to get the real message from the steganographic image. This method is much safer compared to LSB as it requires an algorithm and a key to cut a small message from a steganographic image. Therefore, users choose this method for its safety as it requires both algorithm and key despite steganographic image. This LSB-like method has diets such as image destruction in terms of image processing and compression. Some people choose this method because of the large amount of extra effort a person who does not have a steganographic key and algorithm must go through to get the message across. Even if White Noise Storm provides additional security in message retrieval it is possible that the LSB may have image damage due to image processing.

D. Algorithms and transformation

The LSB conversion process does not work if there is a type of compression applied to the steganographic effect image for example JPEG, GIF. JPEG images use discrete cosine transform in compression. Since cosine values cannot be calculated exactly, DCT is a loss of variable pressure. And repeated calculations with limited finances bring rounding errors to the final answer. The difference between the amount of actual data and the amount of data returned depends on the method used to calculate the DCT.

A sophisticated way to hide the secret inside the image is the use and modification of different cosine modifications. A different cosine conversion is used by the JPEG compression algorithm for converting blocks of 8 x 8 consecutive image pixels, into 64 coefficients of DCT each. Each DCT F (u, v) component of the 8 x 8 block pixel block f (x, y) is usually indicated by:

After calculating the coefficients, the following measurement function was performed:

1- Where *Q(u, v)* is a 64-element quantization table.

2- A simple pseudo-code algorithm to hide a message inside a JPEG image

3- **Input:** message, cover image

4- **Output:** steganographic image containing message **while** data left to embed do

5- get next DCT coefficient from cover image **if** DCT 6= 0 and DCT 6= 1 then

6- get next LSB from message

7- **replace** DCT LSB with message bit

8- **end if**

9- **insert** DCT into steganographic image

10- **end** while

11- Initially there was the idea that steganography would not be possible with JPEG images, because they use the lost pressure that leads to parts of the image to change. One of the main features of steganography is that the details are hidden in the obsolete parts of the object. As unwanted fragments were left out when using JPEG, it was thought that the hidden message would be destroyed. Even if the message is not kept in some way it will be difficult to embed the message without some noticeable changes. This is mainly due to the heavy pressure applied.

12- Compression algorithm features have been used to create a steganographic algorithm for JPEGs. One of the features of JPEG that is exploited to make changes to the image is to make it invisible to the human eye. During the DCT transition phase of the compression algorithm, in the case of random data collection errors that do not appear easily. Although this asset separates the algorithm as a loss, the same asset can also be used to hide messages.

13- It is neither possible nor possible to embed details in an image using lost compression, as compression will damage all information in the process. It is therefore important to know that the JPEG compression algorithm is divided into lost and non-lost categories. The DCT and quantization phase are part of the loss phase, while the Huffman coding used to continue compressing data is not lost. Steganography can occur between these two stages. Using the same LSB insertion principles a message can be applied to the most important pieces of coefficients before entering the Huffman code. By embedding data in this section, in the conversion domain, it is very difficult to find it, because there is no visual domain.

Masking and Filtering

Hiding and filtering is a method of steganography used in limited images. The concealment and filtering method works best with 24 bit images and grey. They contain the same hidden information in watermarks on the real page. They are called digital watermarks because of this.

Hiding an image changes the image. To ensure that this change is not available, it is done in small quantities. The concealment and filtering process usually begins with image analysis. Then important areas are found, where the hidden message will be collected at the top to cover the image and finally the data is entered into that area. This method incorporates private information into more important areas than just hiding it in the audio category.

This method expands image information by hiding private data over the original data as opposed to hiding details within the data. This creates some controversy among experts that it is definitely a kind of Hidden Information but it may not be the technical Steganography. In this paper it is considered a steganography procedure. Hiding and filtering methods are safe from image manipulation. While masking changes the visual properties of an image, it can be implemented in such a way that the human eye does not see the disorder.

Compared to LSB, mask masking is a solid method as they are protected from image manipulation. These hidden images go beyond the caption, compression and a certain amount of image processing. Hiding the embedding of information in key areas so the hidden message is more closely related to the cover image than the hidden level of sound. Therefore, it is better than LSB for example JPEG lost images. Poor quality of image retrieval is a major problem.

STEGANALYSIS

This section includes the most well-known and important steganography techniques developed and helps to better understand the process. Chi square attack is a very simple and popular way to test the strength of a security system from an attack. Chi-square Attack works effectively for LSB steganography of local images and JPEG images. The square test of chi [9,14] is used to detect hidden messages using the concept of dependence on both. It is based on the feasibility analysis of the steganographic image after the information has been entered into it using the LSB method and then compared the probability analysis of the first image to see the differences between them. If the difference occurs near zero, it means that there is no information within the image otherwise it means that the image contains details. It is very reliable for consecutive embedded messages. In future ongoing activities it was developed to receive randomly dispersed random messages.

Fredrich et al. upgraded Raw Quick Pair (RQP) for 24-bit colour images. He later developed this in both grey scales and colour schemes. Fredrich et al. set the RS algorithm for steganography to detect LSB embedding in rated 8-gray images and 24bit colour images. In this process the total number of image pixels separated by four pixels (2 × 2 blocks) of groups are combined. Discrimination function f (.) Is used in these groups to determine the softness of the groups.

1. f (G) = f (x1, x2, ……, XNA) =: x1, x2, ……, XNA by group pixels G.
2. Also, three fixed function functions are applied to the pixel x value.
3. F1 (x): 0 ↔ 1, 2 2 3… 254 ↔ 255
4. F-1 (x): −1 ↔ 0, 1 ↔2… 255 ↔ 256
5. F0 (x): Copyright function
6. Operation F1 (x) and F-1 (x) are used in a group of pixels based on Mask M n-Tuple with values of -1,0,1. if the values of the four G-pixels are 13, 23, 46, 64 and M = (1, 0, 1, 0), then FM (G) = (F1 (13), F0 (23), F1 (46), F0 (64)). Defined function, mask and function are applied to a group of pixels and are distributed by the following groups:
7. General groups: G ∈ R ⇔ f (F (G))> f (G)
8. Individual groups: G ∈ S ⇔ f (F (G)) <f (G)
9. Inactive groups: G ∈ U ⇔ f (F (G)) = f (G)
10. This approach is based on analysing how the number of individual and general groups changes with the increase in message lengths placed on an LSB aircraft. Message size, reduces the difference between RM and S-M and ****** difference between RM and SM. This behaviour difference is used to detect a hidden message from a steganographic image.
11. Westfeldt et al. propose a process based on statistical analysis of the Pairs of Values using square attacks alternating during message embedding. The concept of mathematical analysis is to compare the theoretically expected frequency (i.e. mathematical interpretation of the two frequencies since the first cover is not available) distribution in steganography and sample distribution of the steganographic method. To find out the differences in the distribution of the use of the aforementioned calculation:
12. The probability of embedding is decided by calculating the p-value defined below:
13. This p-value is calculated for any sample from the values examined which usually starts from the beginning of the image and gets amplified for each measurement.

TAXONOMY OF STEGANOGRAPHIC TECHNIQUES

There are many ways to separate steganographic techniques. These methods can be classified according to the type of covers used for private communication. Another option is to customize such methods according to the type of cover used already in the embedding process. The second method is adopted for this function, although in some cases direct separation is not possible. In general, the embedding process can be described as follows

Let C show the cover carrier, and C ~ steganographic image. Allow K to represent the optional key (such as seeds used for encrypting a message or to produce duplicate sound, which can be set to {φ} easily), and M for the message to be sent. After that, it represents the embedded message and Ex represents the extracted message. To distinguish between different steganographic techniques in a broader sense, one must look at both the image converter and those that change the image file format. However, file format conversion is not very powerful. An important issue that will be discussed here in the main role is the pressure that often plays when it comes to deciding which steganographic algorithm is best. Although lost reduction methods result in smaller image sizes, they increase the chances of loss which is part of the embedded message because the remaining image data must be removed from these methods. Active compression does not compress the image file too much. As a result, researchers have come up with various steganographic algorithms that are associated with such types of stress. Steganographic techniques convert image encryption files into the following

- Local domain
- Change domain
- Spread spectrum
- Mathematical methods
- Distortion strategies

Steganographic techniques that change the image file format include file embedding and palette embedding. In addition, there are strategies that transform the elements in the visual image including: Image processing process; and the process of converting an image object. Finally, there is a special type of domain-changing strategy called adaptive steganography technique, which we define and completeness. The following section describes each steganographic method in detail.

1- Spatial Domain Technique

Spatial domain steganographic methods, also known as replacement techniques, are a group of simple strategies that create a cover-up in parts of the cover image where the changes may be small compared to the human viewing system (HVS). LSB) image data. This embedding method is since the most important fragments in an image can be considered as random sound, and therefore do not respond to any changes in the image.

2- Transform Domain Techniques

Conversion domain embedding can be defined as the domain of embedded strategies in which multiple algorithms are developed. The process of embedding data on a common signal domain is much stronger than the embedding principles that apply to a time domain. It is worth mentioning that most of the solid steganographic systems today operate within the transformation domain. Domain conversion techniques are more advantageous than LSB techniques because they hide information in image areas that are less open to compression, blocking, and image processing. Some dynamic domain strategies do not seem to depend on image format and may result in non-lost and lost format conversion. JPEG file format is the most common image file format on the Internet due to the small size of the resulting images obtained using it.

3- Spread Spectrum Technique

The spectrum broadcast on radio communications conveys messages below the audio level at any given frequency. If employed with steganography, the broadcast spectrum can interact with the cover image as sound or attempt to insert artificial sound into the cover image.

• Photo cover as sound the system that handles cover image as sound can add a single value to the image. This value must be transferred below that noise level. This means that the channel size of the image changes significantly. So, while this number can be a real number, in fact, the difficulty of finding the real number reduces the value to one. To allow for more than one transfer, the cover image must be broken into sub-images.

When the images under the cover are tiles, the process is called direct sequence spread spectrum steganography. When the images under the cover contain different points that are distributed over the cover image, the process is called frequency-hopping spread-spectrum steganography. These methods require you to search for a carrier image to get details

• Fake counterfeit This method shows that hidden information is spread across the cover image which is why it is difficult to detect. Spread spectrum image steganography described by Marvel et al, integrated spectrum interaction, coding error management, and image processing to hide information in images.

4- Statistical Methods

Also known as model-based techniques, these techniques often alter or alter image mathematical properties in addition to keeping them in the embedding process. These modifications are usually small, so it is possible to take advantage of human weakness in detecting a wide range of enlightenment. This process is done by simply changing the cover image to make a kind of significant change in the mathematical symbols when passing “1”, otherwise leaving it unchanged. To send multiple fragments, the image is divided into images below, each corresponding to a single message.

5- Distortion Techniques

Distortion techniques require knowledge of the first cover image during the comprehension process where the decoder works to check the difference between the original cover image and the curved cover image to restore the confidential message. The encoder, on the other hand, adds a sequence of changes to the cover image. Therefore, the data is defined as the retention of signal distortion Using this method, a steganographic object is created using a sequence of image conversion of the cover. This sequence of conversions has been selected to match the secret message needed to convey the message embedded in the false selected pixels. If the steganographic image differs from the cover image in the given message pixel, the bit message is “1.” Otherwise, the small message is "0." The encoder may change the value of the “1” value pixels in such a way that the imagery architecture is unaffected (unlike most LSB methods). However, the need to post a cover photo limits the benefits of this approach. As with any steganographic procedure, the cover image should not be used too often. If the attacker distorts the steganographic image by cropping, rotating, or measuring, the recipient can easily see the conversion.

ACKNOWLEDGMENTS

An acknowledgement to Academy of Scientific Research and Technology for its contributing constructively in completion of this paper

REFERENCES

[1] A. Cheddar, J. Condell, K. Curran, and P. M. Levitt, 3, pp. 727–752, 2010.

[2] R. Chermoula, M. Kharrazi, and N. Memon, Berlin Heidelberg, 2004, pp. 35–49.

[3] E. E. A. Elgabar and H. A. A. Alamin, "Comparison International Journal of Soft Computing and Engineering (IJSCE), vol. 3, no. 4, pp. 79–83, 2013.

[4] L. Zhang, J. Wu, and N. Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Conference on Information Assurance and Security, 2009, pp. 61–64.

[5] P. Ajit and K. Chouhan, "A Study and literature Journal of Computer Science and Information Technologies (IJCSIT), vol. 6, no. 1, pp. 685–688.

[6] P. B. Kutade and P. S. A. Bhalotra, "A Survey on Various Approaches of Image Steganography," International Journal of Computer Applications, vol. 109, no. 3, pp. 1–5, 2015.

[7] G. J. Simmons, "The Prisoners' Problem and the Proceedings of CRYPTO '83, springer, 1983, pp. 51–67.

[8] N. Akhtar, P. Johri, and S. Khan, "Enhancing the Security and Quality of LSB Based Image Conference on Computational Intelligence and Communication Networks, 2013, pp. 385 – 390.

[9] M. S. Subhedar and V. H. Mankar, "Current status Computer Science Review, vol. 13–14, pp. 95–113, 2014.

[10] D. Salomon, Coding For Data And Computer Communications. California State University: Springer, 2005.

[11] N. F. Johnson and S. Jajodia, "Exploring 31, no. 2, 1998.

[12] M. Mishra and F. L. D. M. C. Adhikary, "An Easy yet Effective Method for Detecting Spatial Domain Computer Science and Business Informatics, vol. 8, no. 1, pp. 1–12, 2013.

state-of-the-art overview," IEEE Signal Processing Magazine, vol. 17, no. 5, pp. 20–46, 2000.

[14] S. Katzenbeisser and F. A. P. Petitcolas, Information
Hiding techniques for stegnography and digital watermarking. Artech House, Inc. Norwood, MA, USA, 2000.

[15] P. C. Mandal, "Modern Steganographic technique : Science & Engineering Technology (IJCSET), vol. 3, no. 9, pp. 444–448, 2012.

[16] C. Kurak and J. McHugh, "A Cautionary Note On Security Applications Conference, Eighth Annual, 1992, pp. 153–159.

[17] F. Petitcolas, "The information hiding homepage." [Online]. Available: http://www.petitcolas.net/steganography/image_do wngrading/.

[18] V. M. Potdar and E. Chang, "Grey Level Modification Steganography for Secret International Conference on Industrial Informatics, 2004, pp. 223 – 228.

[19] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9–10, pp. 1613–1626, 2003.

[20] Xinpeng Zhang and S. Wang, "Vulnerability of pixel-value differencing stegnography to histogram Pattern Recognition Letters, vol. 25, no. 3, pp. 331–339, 2004.

[21] J. C. Joo, H. Y. Lee, and H. K. Lee, "Improved Steganographic Method Preserving Pixel-Value EURASIP Journal on Advances in Signal Processing, vol. 2010, pp. 1–13, 2010.

[22] C. H. Yang, C. Y. Weng, H. K. Tso, and S. J. Wang, Journal of Systems and Software, vol. 84, no. 4, pp. 669–678, 2011.

[23] Y. P. Lee, J. C. Lee, W. K. Chen, K. C. Chang, I. J. with quality recovery using tri-way pixel-value 214–225, 2012.

[24] G. Swain and S. K. Lenka, "Steganography using two sided , three sided , and four sided side match pp. 127–133, 2013.

[25] B. Chen and G. W. Wornell, "Quantization Index
Digital Watermarking and Information Theory, vol. 47, no. 4, pp. 1423–1443, 2001.

[26] T. D. Kieu and C. C. Chang, "A steganographic
Expert Systems with Applications, vol. 38, no. 8, pp. 10648–10657, 2011.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord "Format" pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.