REVIEW OF VITAL TECHNIQUES FOR HIDING CONFIDENTIAL DATA USING IMAGE STEGANOGRAPHY

[1]Tanu Garg,[2]Kamaldeep Joshi, [3]Rainu Nandal, [4]Gaurav
[1]M.TECH Student,[2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor
University Institute of Engineering Technology, Maharashi Dayanand University, Rohtak,India
[4]Department of Computer Science & Engineering, School of Engineering Sciences & Technology, Jamia Hamdard, New Delhi, India

Abstract—The quick advancement in the exchange of information through internet made it easier to exchange information exact and faster to the receiver. Security of data is one of the huge components of information technology and communication. Steganography is a term used for information hiding and it is an art of hidden writing. In steganography we hide information with a multimedia carrier i.e. image, text, audio, video files, etc. So, that observer cannot find the hidden information which we want to send to the receiver. Steganography main objective is to provide robustness, detectability, capacity of hidden data due to which it differs from other techniques such as watermarking and cryptography. This paper proposes a various technique used to hide information on image by an image steganography. In image steganography we hide our secret data in image so that the observer cannot feel its existence. Image steganography strategies are as of late been useful to send any secret message in the secured image carrier to anticipate threats and attacks, though it does not give any sort of opportunity to programmers to discover the secret technique. Image steganography is efficient and better type than other types of steganography. In image steganography data can be secured by the use of spatial and frequency domain. The difference in both is that in frequency domain first information is embedded in the changed picture rather than direct pixel and after that picture is transformed to spatial domain. There are many steganography algorithms in which each has its own advantages and limitations in terms of security and complexity. Critical analysis depends on the type of cover object used, domain of algorithm and imperative properties that are utilized as evaluative measures for Steganographic techniques.

Keywords—Steganography, Information hiding, Cryptography, Spatial domain, Frequency domain, Interpolation

1. INTRODUCTION

As the increased use of internet one of the beneficial factor of communication to be the information security [1]. Cryptography used only for securing the communication by encrypting or decrypting our data. But if some unusual person decrypts that code, then there will be no security system. So, another term proposed with cryptography i.e. steganography in which we not only secure the communication, but also the existence of the message. As another term watermarking in which we try to prevent our hidden information by contrary of transforming hidden message, which is part of cover data, but in steganography we did not do this we make sure that no one knows the existence of the message [2]. Steganography can be used as both legally and illegally. Good user uses it for securing communication while hacker uses it illegally to gain other data. Fig. 1 shows different disciplines of information hiding [3]. Table 1 shows a comparison between steganography, cryptography, and watermarking [4].

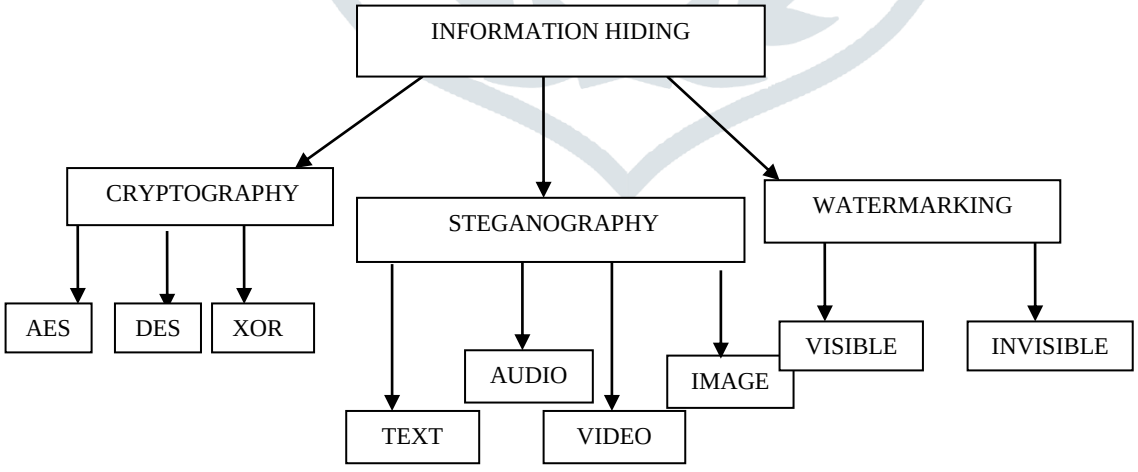

FIGURE 1: Disciplines of information hiding

TABLE 1: Comparison between steganography, cryptography, watermarking

Criterion	Cryptography	Steganography	Watermarking
Technique	Substitution, RSA, AES	LSB, DCT, Histogram, DFT	Compensated prediction
Result	Cipher-Text	Stego-File	Watermarked-File
Capacity	High	Differ as different technology	Depend on size of hidden data
Strength	Hide message by altering message	Hide message without altering the message	Extended information

Carrier	Text/image files	Any digital media	Image/audio files
Detection	Not easy to detect	More secure than other two	Not easy to detect

2.History of Steganography

In ancient time, this technique was first time used in Greece from the 5th century. Greece people hide information on the head of their salvation. First, they cut the hair of their slave then write the message and then wait until hair grew and message hidden. Then send salve to another place and they decrypt it by slaves his hair. In 1600s, steganography technique is used by Sir Francis Bacaon in a face variant encoding. The Italian Jerome cardan five hundred years ago again discovered an approach for hidden data. In this a paper mask is taken with a hole in it and shared with two people, then paper is placed on a blank sheet and by using holes, secret message is written by the sender and then take out the mask and fill the blanks so that message appear as simple text. This method, known as Cardan Grille method [5]. When World War 2 was going on, steganography technique is used. By the help of invisible ink information was written on paper and in the normal light paper looked hollow for a normal person. Finally, by using liquids such as alcohol, juices information read out. First, we heat the moist paper in the liquid so that they became darker and message written are shown to receiver eyes.

3. Steganography Method:

This section provides an overview about the steganography types in which hiding information in different multimedia carrier. T. Morkel proposed about different types of steganography. In Text steganography, the secret message is hidden in a text. There are many techniques such as we decide every English alphabet is changed to its every preceding letter. In Audio steganography, a secret message is hidden in the audio file. In Video steganography, a secret message is hidden in a video file. Image steganography is a term used to hide secret information into cover image without changing image and offer security so that no unusual person can find the hidden message.

Anjli Tiwari proposed an example about the image steganography technique in Figure 2. Let's "M" and "N" are two persons who try to talk secretly. As, there all talk was acknowledged by the "O" using an Internet service provider or router, etc. As "M" to send a secured message "m" to "N" for this, "M", put in covers objects "c", and obtains a stego-object "s". The stego-object "s" is then sent. Cover – object is defined as an object used as carrier to embed messages in it. Stego- object is defined as an object which carries the hidden message.

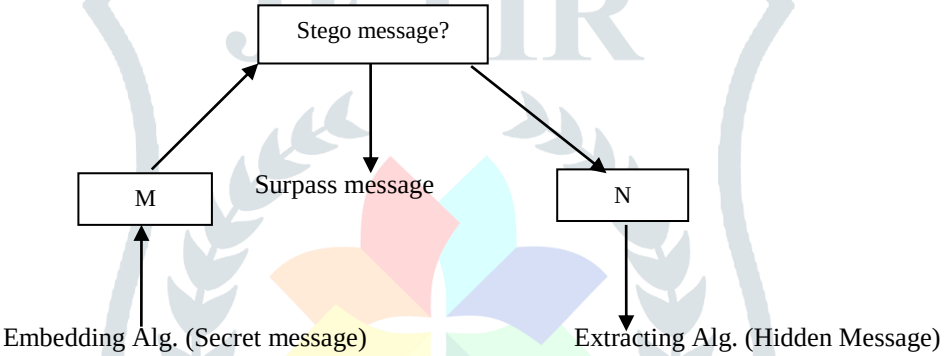

FIGURE 2: Image Steganography Technique

Section 3.1 discusses about how steganography can be used to hide data in the image. Section 3.2 discusses spatial domain technique which describes various techniques such as LSB, Modification of LSB, Pixel based difference, Histogram based and also discuss about interpolation method. Section 3.3 discusses frequency domain technique such as DCT, DFT, and DWT.

3.1 Steganography to hide data

Steganography can be used by using simple feeding into window OS command window. In this we have taken a one original image named as koala.jpg and in this we add one text file named as tanugarg.txt by using comedy we combined both file and get a hide.jpg file. The following code we used as "copy /b original.jpg + tanugarg.txt=hide.jpg". What does this code does it append the data that found in" tanugarg.txt" into the image "original.jpg" and produced the stego-image "hide.jpg" [6]. Figure 3 shows that how data embedded in image file using OS command window.

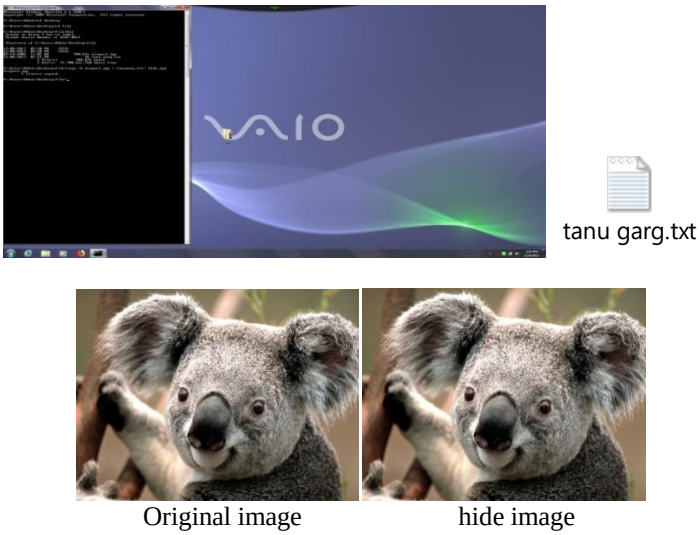

FIGURE 3: Data embedded in image file using OS command window

3.2 Steganography using spatial domain

Spatial domain technique is used for information hiding in which we changed bits directly into image pixel values [7]. In this effect of message is not seen on the cover image secret. N.K. Mittal proposed a various different methods for spatial domain technique.

LSB is one of the simplest methods for hiding data. In this technique, the least significant bits of image pixels are used for hiding messages. As if we change the last bit, then it does not make more difference in the image and the unusual user cannot detect it only by the view [8]. It is easy to use and implement and in this high message payload is there and there is no chance of degradation of the quality of the actual image.

Example (Message): 010100
Pixels: (00101001 00100001 10010100
10001101 11001001 01001000)

Result: (00101000 00100001 10010100
10001101 11001000 01001000)

Khan Muhammad et al. Proposed approaches for LSB method. In this he discussed LSB matching (LSB-M) in which by adding +1 or -1 in given pixel it changes the pixel, then compare message bit with LSB of pixel if not same, then keep the value of a pixel in the range 0-255. In Cyclic LSB we disseminate the message in the entire host picture, utilize stego shading cycle strategy for cover image. Stego shading cycle hide information in various channels of the cover image. The 1st secret bit in the red channel, 2nd in the green channel, 3rd in the blue channel. In Edge based area pixel can accommodate more secret bit than smooth area and less detectable by HVS. It separates the information into two squares and navigates the pixel beginning from the focal point of the image. In LSB-MR inserts 2 secret bits at one time. 1st secret bit in first pixel and 2nd secret bit is covered up by the connection between pixels in that match [9].

Abbas Cheddad et al. proposed a color palette based steganography in this it exploits the smooth incline change in colors as demonstrated in the color palette. Here LSB was utilized based on their position in the palette record. In this, first they have used BMP (24 Bit) files later they used in GIF files as BMP files are bigger as compared to other formats that make it improper for network transmissions. BMP as well as GIF based steganography apply LSB techniques, while their resistance to statistical counter- attacks and compression are reported to be weak. JPEG images however, were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain. In authors claimed that changes as small as flipping the LSB of one pixel in a JPEG image can be reliably detected.

Jung and Yoo introduced a traditional scaling up method in which it down examined an information picture to ½ of its size and utilized another introduction technique that attention on high speed and low complexity and named as neighbor mean interpolation strategy. It used pixel value of neighbor and calculated their mean value and inserted in blank pixel. Then sampled the result back to its original dimension [10-11].

EX:

140	160
190	188

Original 2*2block

140	150	160
165	152	167
190	156	188

Interploated block

d=0; 150-140=10; 165-140=25; 152-140=1

n=0; $[\log_2 |10|] = 3$; $[\log_2 |25|] = 4$; $[\log_2 |12|] = 3$;

Secret bits: 1001010011……..

Decimal value 100=4, 1010=10, 011=3

140	154	164
175	155	167
190	156	188

Stego 2*2 block

Palette based image steganography is like the generally utilized LSB strategy for 24 bit color pictures (or 8 bit gray scale pictures). After the palette colors are arranged by luminance, it inserts the message into the LSB of records indicating the palette color. Recovery of the message is basically accomplished by choosing similar pixels and gathering the LSBs of all records to the requested palette [12].

Pixel value difference was analyzed that human eyes can rapidly watch slight change in smooth regions, while the change in edge zone are done not be known by unusual individual. In PVD, the quantity of inserting bits is calculated by the distinction between the pixel and its neighbor. The bigger the distinction sum is the more secret bits can be inserted into the cover picture. Usually, PVD based approaches can achieve more imperceptible results compared with those typical LSB-based approaches with the same embedding capacity. However, based on extensive experiments and analysis, we find that most existing PVD based algorithms perform bad to resist some statistical analysis even with a low embedding capacity [13].

Histogram shifting method is utilized for graphical portrayal of picture. It shows the pixel value and thickness at a specific pixel. In this Pairs of peak points and zero focuses are utilized for accomplishing low installing distortion to give low information hiding limit. In histogram the most elevated esteem is called maxima and the least esteem is called minima. At the point when the pixel esteem is adjusted for implanting

process it doesn't cross the minima and maximum limit. The quantity of the pixels constituting the top in the histogram of a cover picture is equivalent to the hidden limit [14].

Spread spectrum: The center of spread spectrum image steganography (SSIS) is a spread spectrum encoder. These tactics work by adjusting a tight band signal over a carrier. The carrier frequency is persistently moved utilizing a pseudorandom noise generator feeded with a mystery key [15]. To extricate the inserted message, the receiver must utilize a similar key and noise generator to turn on the correct frequencies and demodulate the actual signal. An easygoing eyewitness won't be capable even to identify the concealed correspondence, since it is below the noise level.

Saher manaseer proposed a new method that was standard LSB and Condition Based LSB [21]. In this technique LSB changes the last bit by corner to corner. This technique changes the last bit or the second minimum last bit in light of the condition as takes after: If the most significant bit is 1, the calculation changes the second least Significant bit. Something different, the estimation changes the last bit. This system is more secure contrasted with others due with depending upon the reference of data; it hides the reference not the actual data.

KamaldeepJoshi et al. proposed a LSB steganography method and investigate the PSNR and MSE of LSB information hiding procedure based on various message sizes [22]. The proposed LSB scheme takes the first LSB bit of the image and the first message bit from the message lattice and inserts the message into the first image. After addition of first message bits, pixel area of picture and message is increased by one. This procedure consistent itself till the message length isn't equivalent to zero. In this PSNR is more for the short message and less in case of long message size and MSE is less for the short message and more in case of long message size.

Kamaldeep Joshi et al. proposed a new method that mixes the benefits of 2 bit LSB and XOR operation [23]. In this first we are XORing the 8th, 1st bit of data and 7th, 2nd bit of data after these two bits are obtained. These obtained bits are supplanted at the LSB position. It is secured strategy as though any individual become acquainted with about secret message and it takes the LSB position bit at that point there are no odds of getting message as it isn't actual message. At the point when this technique was contrasted and other existing strategies, it indicates improvement in the imperceptibility and message limit.

3.3Steganography using frequency domain

There was need of an emerging new algorithm due to the performance of their ancestors and quick improvement of data innovation and need of further development security framework. As an LSB embedding component was a major accomplishment to be found, but it can be detected by unintended user. So, there was need to generate more secured method due to which frequency domain technique is developed. In this technique we utilize domain specific qualities of picture to insert information on it and to perform it the picture initially changed in the area and first information is embedded in the changed picture rather than direct pixel and after that picture is transformed to spatial domain [16]. As they are exposed to compression, cropping, image processing.

DCT (Discrete cosine transformation): The description of DCT technique we transform the picture from spatial to frequency area and isolates the picture into spectral sub-groups as indicated by its quality, i.e. low, center and high frequency parts accordingly it make easier to pick the band in which hidden picture is to be embedded. Amritpal singh et al. revealed that mostly middle frequency band is chosen as if we embed information in the middle, then it does not scatter the information on all parts of the image.

Equation of DCT is:

$$F(u,v) = \frac{1}{4}C(u)(v)\sum_{x=0}^{7}\sum_{y=0}^{7}\left(\mathrm{f(x,y)} * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)u\pi}{16}\right)$$

DCT is used in the JPEG Compression algorithm to change progressive 8*8 pixel piece of a picture into 64 DCT coefficients each in the frequency domain. It's coefficient F (u,v) is calculated above.

$$F(u,v) = \frac{F(u,v)}{Q(u,v)})$$

Where Q (u, v) is a 64-component quantization table. The hidden message is inserted into repetitive bit, i.e. LSB of quantized DCT coefficients.

Raja et al. discussed fast fouier transform method, but it introduced round- off errors, it was not benefited for hidden information .So, Mckeon utilized 2D DFT technique to give fouier based steganography.It was similar to DCT technique, but it used fouier transformation instead of cosine. In this frequency domain is used for insertion of hidden messages and used in covert spatial component to frequency. DFT of spatial value f (x, y) for an image of size P*Q is given as

Equation of DFT is:

$$f(u,v) = \frac{1}{\sqrt{\mathrm{PQ}}}\sum_{x=0}^{P-1}\sum_{y=0}^{Q-1}\left(\mathrm{f(x,y)}e^{-12v}\frac{ux}{P}+\frac{vy}{Q}\right)$$

But, they used inverse discrete fouiertransformation to change frequency parts of each pixel value to spatial domain instead of x and y in above equation they used u and v respectively. In this each pixel is transformed into 2 parts, i.e. real and imaginary part. After this they applied IDFT to covert frequency to spatial domain.

As for Steganography another transformation technique was introduced discrete wavelet transform. S. R. Yadav et al. introduced this asa wavelet is a little wave which sways decays in time domain. In this data is put away into wavelet coefficients as opposed to changing of bits of real pixels in the picture. It additionally performs local analysis and multi resolution investigation. The DWT-based method is still in its earliest stages. Abdelwahab and Hasan proposed a DWT space in which both secret and cover pictures are deteriorated. Each of which is divided into disjoint 4*4 pieces. The DWT parts into 2 sections high and low frequency. The data about the edge segment is in high frequency and low frequency is part in high frequency parts [17].

The IWT- based is another approach that has some difference than DWT.Since the discrete wavelet transform permits autonomous preparing of the resulting parts without significant discernible connection between them, henceforth it is required to make the procedure of impalpable inserting more powerful. Be that as it may, the utilized wavelet channels (and furthermore alternate channels like DCT, FFT) have floating

point coefficients [12]. In this way, when the information comprises of arrangements of whole numbers (as for the situation for pictures), the subsequent separated yields never again comprise of whole numbers, which doesn't permit perfect reconstruction of the original picture. Some of the advantage and disadvantages of frequency transform domain [12] :

Advantage of frequency transform domain:
1. Higher flexibility and security for hiding data.
2. Less shot for expulsion or loss of concealed information.
3. Data is spread over all whole images.

Disadvantage of frequency transform domain:
1. Higher mathematical complexity.
2. Low embedding capacity.
3. Cautious determination of implanting coefficients is required.

4. Conclusion

In this paper, we have talked about the steganography and for the most part image steganography methods. Each strategy has its own significance and use for concealing the information in the picture. After the investigation of the all procedures it is anything but difficult to choose a specific one for hiding data. The investigation demonstrates that the transform domain approaches are best for the data stowing away with bring down information limit and higher multifaceted nature while the spatial area is best for constrained many-sided quality frameworks. In this we have discussed the difference between cryptography, watermarking, steganography. We have also discussed about an combined technique that mixes the benefits of 2 bit LSB and XOR operation. For further work we can combine image steganography technique with some another cryptography technique that provides more security for hiding the data. We can make technique which can secure more than one bit at a time. In neural network also we can use these techniques for calculation purpose.

REFERENCES

[1] T. Morkel and J.H.P. Eloff, " Exploring simple steganography", Information and Computer Security Architecture Research Group, Department of Computer Science, University of Pretoria, Volume 87, Issue 2, pp. 26-34, 2005

[2] S. R. Yadav, A. Tiwari and N.K. Mittal, "Image steganography technique", International Journal of Engineering and Innovative Technology, Volume 3, Issue 7, pp. 19-23, 2014

[3] A. Cheddad and J. Condell, "Image Steganography survey and analysis", Faculty of Computing and Engineering, University of Ulster at Magee, Volume 90, Issue 12, pp. 727-752 , 2010

[4] H. V. Desai, "Difference between steganography, Cryptography, Watermarking", Journal of global research in computer science, Volume 3, Issue 12, pp. 33-35, 2012

[5] P. Moulin and R. Koetter, "Data-hiding codes", Proceedings of the IEEE, Volume 93, Issue 12, pp. 2083–2126, 2005

[6] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, Volume 5, Issue 3, pp. 75-80, 2001

[7] K. Bailey and K. Curran, "An evaluation of image based steganography methods", International Journal of Engineering and Computer Science, Volume 30, Issue 1, pp. 55-88, 2006

[8] L. Zhi and S. A. Fen, " LSB Image Steganography", Vehicular Technology Conference IEEE, Volume 3, Issue 5, pp. 2113-2117, 2004

[9] K. Muhammad and M. Sajjad, " Modification on LSB method", Springer Science, Volume 22, Issue 1, pp. 647-654, 2015

[10] Ki. H. Jung and Kee. Y. Yoo, "Data hiding method using image interpolation", Computer Standards & Interfaces, Volume 31, Issue 2, pp. 465-470, 2009

[11] Ki. H Jung and Kee. Y. Yoo, "Steganographic method based on interpolation and LSB substitution of digital images", Multimedia Tools Application, Volume 74, Issue 5, pp. 2143-2155, 2014

[12] A. Singh and S. J. Singh, " Image steganography technique", International Journal Of Engineering and Computer Science, Volume 3, Issue 7, pp. 7341-7345, 2014

[13] D.C.Wu and W. H. Tsai, "Pixel value difference method for image steganography", International Journal of Engineering and Computer Science, Volume 24, Issue 6, pp. 1613-1626, 2003

[14] K. Qazanfari, R. Safabakhsh, "A new steganography method which preserves histogram: generalization of LSB", International Journal of Engineering, Volume 0007, Issue 7, pp. 90-101, 2017

[15] X. Li. Wang, "Spread spectrum technique for Steganographic Method", Information Science, Volume 177, Issue 15, pp. 3099-31091, 2007

[16] D. Frith, "Steganography approaches, options and implications, Network Security", International Journal of Engineering and Computer Science, Issue 8, pp. 4-7, 2007

[17] A. A. Shejul and U.L. Kulkarni, "A DWT based Approach for Steganography using Biometric", International Conference on Data Storage and Data Engineering, Volume 152, Issue 4, pp. 39-43, 2010

[18] T. Ahmad, AL. Tanni and AL. Issa, "A Novel steganographic method for gray level images", International Journal of computer, Volume 3, Issue 3, pp. 102-106, 2009

[19] M. Katoch and R. Jaswal, " Techniques of image steganography ", International Journal of advanced research in computer and communication engineering, Volume 5, Issue 4, pp. 827-830, 2016

[20] D. Garg and G. Sharma, "Applications of steganography in information hiding", International Journal of advanced research in education and technology, Volume 3, Issue 1, pp. 12-14, 2016

[21] S. manaseer, A. Aljawawdehand and D. Alsoudi, "A new Image steganography depending on reference & LSB", International Journal of Applied Engineering Research, Volume 12, Issue 9, pp. 1950-1955, 2017

[22] K. Joshi, R. Yadav and S. Allwadhi, "PSNR and MSE based investigation of LSB", Proceedings of the IEEE Conference, 2016

[23] K. Joshi, R. Yadav and G. Chawla, "An Enhanced method for data hiding using 2 bit XOR in image steganography", International Journal of engineering and technology, Volume 8, Issue 6, pp. 3043-3055, 2017