International Journal of Engineering & Technology, 7 (3) (2018) 1024-1033

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.8940
Research paper

Understandable Steganography

InduMaurya[1]*, S. K Gupta[2]

[1]Research Scholar, CSE Deptt. B.I.E.T Jhansi
[2]A. P., CS&E Deptt., B.I.E.T Jhansi
**Corresponding author E-mail:indumaurya42@gmail.com*

Abstract

For hiding information in a digitalized object Steganography is an important technique. It is a special kind of scientific technique which involves the secret information communication inside suitable cover objects of multimedia like image files, audio or videos. The embedded data and its existence are hidden with the help of Steganography. It is a method of hiding data which has enormously improved the security level of confidential data with the help of special hiding mechanism and is considered as remarkable achievement in the computational power. The main aims of Steganography are; capacity of concealed data along with its robustness, lack of detection etc. These are some of the additional features which make it distinguishing from other older techniques like watermarking as well as cryptography. In this research paper, we have surveyed Steganography of digital images and cover the basic and key concepts. In spatial representation the development of image Steganographic methodology in the format of JPEG, along with that we will also debate on the modern developments as far as Steganography is concerned.
For increasing Steganographic security, specifically used approaches are shortlisted and the developments made after investigations are also presented in this paper.

Keywords:*Digital Image; Steganography; Domains: Spatial and Frequency; Information Security; Information Hiding*.

1. Introduction

Steganography is a Greek word which means "covered form of writing". Through many years the technique has been in use. It is expected that in the 5th century BC, when slave's head was shaved by Histaiacus, the message was also tattooed at his skull, as his hair grew up the slave was dispatched to convey the message [3] [4]. In the cover objects like text, images, audio or any video Steganography is a special art where data is hidden. The process of hiding data in Steganography has certain methods which additionally incorporate redundant bits of cover medium. A stego file is generated with a help of data embedding process by alternating the redundant bits with that of information from data which is kept hidden. As far as data hiding is concerned, 3(three) essential factors are to be kept in mind are capacity, data amount is inclusive of it which in the cover object can be hidden. The detection of hidden information and alternation amount robustness, the object which is stego can tolerate before all the hidden data is destroyed by adversary [1]. The key purpose of using Steganography is to securely communicate with the third parties keeping privacy ensured and data is kept hidden so that the observer cannot read it. Steganography is a technique where information to be hidden is kept inside an object that us unsuspicious and is sent with high security as no one will be able to know about the secret information or even its existence. A lot of Steganographic uses with which the data is hidden inside an image are simpler to be implemented; it is not easy to break this hidden data so Steganography is used frequently [2].
In our literature we can find so many examples of Steganography [3] [4]. Three of the techniques are linked to each other, Steganography, Cryptography and Watermarking. Steganography and Watermarking are not easy to tease apart particularly for the ones who join from several other disciplines. Such sorts of confusions are sometimes eradicated by Fig. 1 and Table 1. The task mentioned here is seen revolving around Steganography in the images which are digital and no other type of Steganography is discussed here. In this paper we will discuss the Steganographic techniques, their execution, and evaluation and how is this technique better and more reliable as compared to other older techniques.

2. Representing information hiding approaches

Data is hidden with the help of Steganographic techniques inside a cover object as mentioned above. The positive and negative outcomes of this technique are discussed here. Each component's relative significance is generally dependent on the application. [5].

2.1. Information security

Various active and passive attacks might harm the Steganography. On the secret information existence if one can assume the possibility which is lesser as compared to the random guessing in the Steganography systems and Steganography is thought to be much secure in the presence of Steganalytic systems. At the same time we can also argue that Steganography is not much secure technique as far as hiding of a data is concerned.

2.2. Data covering capacity

The hiding capacity for a known data is actually its size which in relative can be concealed to the cover object's size. With higher capacity of data hiding, one can use the small sized cover image for a fixed size data; hence the bandwidth decrease highlights the

Copyright © 2018InduMaurya, S. K Gupta. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

importance of transmission of an object which contains stego image. With the help of embedding the message is turned more short so that one can set image to as little as one can possibly do.

2.3. Perceptual transparency

Inside a cover, message hiding needs cover image's noise distortion. Also it is a key that hiding takes place with no loss of cover object's perceptual quality. In an image when secret information is concealed it must not be allowed further alteration in such a way that it becomes obvious visually that inside an object some information is hidden. As a matter of fact, the stego image obtained must be alike the genuine image so that if two sides are compared one mustn't be able to find out the difference in both, the original image's integrity is to be kept intact [7]. In the applications regarding secret communications, when attacker sees that there is a distortion stimulating suspicion of the data concealed in the stego image, Steganography and its techniques undergo failure even if no proper message is extracted by the attacker. There are some applications in which it is not much important to keep the perceptual transparency of hidden data and they also let much stego image distortion so that the robustness is increased which can hide the capacity or both.

2.4. Robustness

In Steganography, one of the key aims to get is Robustness. It actually is an extent of how difficult it was by a steganalyst to find out the presence or absence of any hidden data. In copyright protection, Robustness is highly important as the attackers will tend to filter any watermarks embedded with images or either destroys them [6] [7].

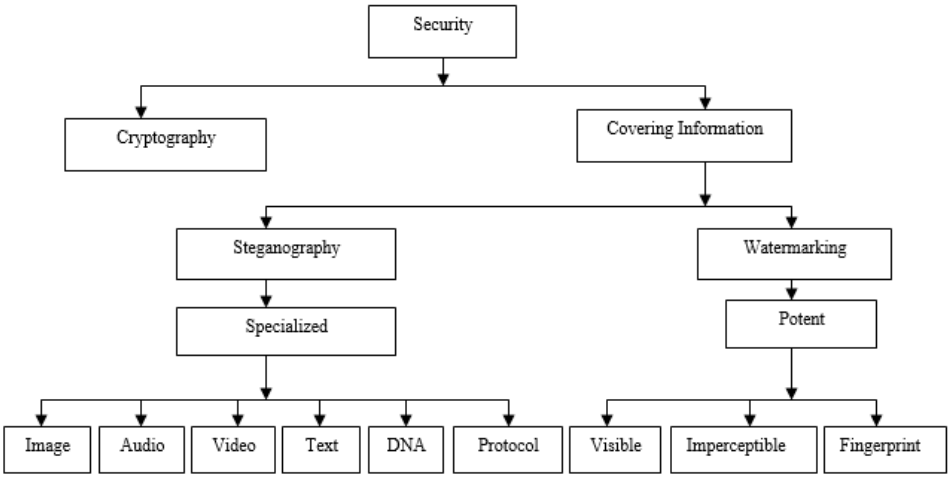


Fig. 1: Information Hiding Disciplines

3. Applications

Steganography has various applications which include printers, communication of secret information and smart IDs copyright security etc. [8] [5].

3.1. Secret transmission/communication

Under different conditions, unwanted attraction is captured while transmitting the cryptographic message. Though cover communication is not publicized by Steganographic messages and as a result it also avoids sender's scrutiny, message along with a receiver. The secret information of military, trading confidentialities, blueprint or any information which is extremely sensitive is passed on keeping the potential attackers unaware.

3.2. Copyright protection

The confidential information regarding copyright or watermark inside an image is likely to be embedded so as to distinguish it as a rational asset [6] [7]. Watermarking scene is used to get it and in this case the watermark is a message with a complicated and complex framework.

In this way the one who intrudes is not able to figure out the information regarding copyright. To find the watermarking there are several available techniques. It can also be seen with the help of watermark that if the image has been modified subsequently [9]. One can get watermarking by correlation, statistically or either by the check of similarity index or by the measurement of characteristics of other quantities to the stego image watermark. The watermark analysis and its insertion to keep the copyright material protected are responsible for the latest interest surge in data embedding as well as digital Steganography.

3.3. Smart Id's

As far as smart ID's are concerned, the personalized data is kept hidden in the image to keep the information private and confidential. In an organization, the resources authentication is accessed by the workers, hence the stealing is identified and crimes are also prevented in this manner. [10].

3.4. Printers

For embedding of the confidential information, some latest printers make use of technique of Steganography. In these kinds of printers like HP printers, inside all the pages, small yellowish dots are placed. All the data which is to be kept confidential is hidden inside these yellowish dots such as, date, time, serial number and stamp etc. In laser printer, the property is made available for the confidential data watermarking [11].

4. Mechanism of image steganography

For the binary images, the Steganography focuses on concealing data in the images which are either colored or grey scale [12] [13]. For a colored image, the component of luminance is equal to the image of grey scale. For hiding data, it is an established fact that the use of grey scale images is more appreciable as compared to colored images [14]. This is due to the correlation disturbances among colored components can highlight some of the data embedded.

The section here is to present an overview of a significant as well as quite famous Steganographic technique for digital images. The image file format which is most popular at internet is JPEG (Joint Photographic Experts Group), GIF (Graphics Interchange Format) and PNG to some extent which is also known as Portable Network Graphics. To exploit the infrastructure of such formats, many techniques were setup with a hope that BMP (Bitmap format) is used for simpler data form.

4.1. Spatial domain

The most common ground for the Spatial Domain Steganography it to modify the image pixel values directly for data concealing. Bits per pixels are used to measure the rate of embedding. In the techniques of Spatial Domain Steganography, a specialist is supposed to modify the confidential information and in a spatial domain, the medium is to be covered. It also incorporates LSBs level encoding. Though this is one of the simplest methods, but it has a huge impact in contrast to the other used methods [15]. Steganography has one of the key grounds to modify the pixel values of images for veiling the data. The data embedded is measured in BPP (bit per pixels). Six major kinds of Steganography are reviewed as under:

4.1.1. Steganography based on least significant bit (LSB)

The LSB of every pixel in the bit technique for the least significant bit in the covered image are substituted with message's binary equivalent which is needed to be kept confidential. The Steganography technique LSB is quite traditional which has a potential to conceal confidential data in a cover image which is digital without the introduction of distortions which are perceptible [14]. The mechanism of this technique is the substitution of the bits with least significance selected randomly in the cover image with the confidential information bits. A secret key may be needed to determine the pixels selection. LSB (the least significant bit) is an easy way to embed any data inside a cover object. The lossless compression is used by some popular image formats like 24 Bit (bitmap), which are utilized for keeping the data confidential. When a resolution image has high quality it becomes easier to conceal data. The best files for concealing information are size 24 Bit images and it mainly is due to their size. Some other file formats can be used like 8 Bit BMP''s or GIF [16].

Due to the limitations in color, the 8 bit images are not much tolerant as far as LSB substitution is concerned. Certain methods with variable levels of success are there which have been presented by the authors of software for Steganography for concealing the data in 8-bit images.
However, there are some discrepancies in such procedure as there is more likelihood of compression of image along with the formatting to the attacks. [17] [18].LSB Steganography for the operations of data concealing can be simply defined by the equation mentioned below:

$$y_i = 2\left\lfloor \frac{x_i}{2} \right\rfloor + m_i \quad (1)$$

In the equation one thing is quite understood that m_i, x_i and y_i represents the i^{th} message bit, the selected pixel i^{th} amount before hiding the data and after hiding the data respectively. There are many tools of Steganography which utilize LSB methodology of Steganography and these include S-tools, Steganos, Steg hide etc which at internet are seen usually. For example, 3 adjacent pixels each of 9 bytes are there with us with encoding RGB [19] (Fig. 2):

10010100 00001100 11001001
10010111 00001110 11001011
10011111 00010001 11001011

Fig. 2

10010101 00001101 11001000
10010110 00001111 11001010
10011110 00010000 11001010

Fig. 3

400 is a number which is represented in a binary way by 110010000 which are concealed in the bits of least significance for the picture. If over LSB of 9 bytes these 9 bits are overlayed, we can get the below mentioned outcomes (Red colored bits and those which are underlined are altered) as mentioned in Fig. 3. Inside the grid, the number 400 was also embedded and there is a change in LSB as per the message which is embedded.

4.1.2. Steganography based on multiple bit-planes

By concealing data in the multiple bit planes, the LSB procedure for concealing the data can be simply extended. The method for non-adaptive data hiding has lessened the stego image's perceptual quality especially if few planes of high bit are taking part in hiding arbitrarily with no employment of any localized asset. In this kind of extension, this is a major defect. BPCS was proposed by Kawaguchi and Eason (bit plane complexity segmentation) for problem solving [20]. With the help of this procedure the cover image being donated in coding system of pure binary codes and will basically be converted into a system known commonly as canonical Gray coding. With the help of it, the breakdown of cover image takes place according to a bit plane into a set of binary images. While each of the candidates is followed by hiding bit plane of canonical Grey coding, the binary image which is analogous is sorted out into chunks of size that are non-overlapping. In this case, $L = 3$ is an option recommended? The image block complexity can be estimated by:

$$\alpha = \frac{k}{2\,x(2^L-1)\,x\,2^L} \quad (2)$$

As compared to a predefined thresholdα_0, it is greater that a chunk is considered as a noise is suitable for concealing the data. In equation (2), the net amounts of white and black borders in the chunk are represented by$k$. At the same time; the data of confidential message is classified into number of data chunks along with its size which is$2^L x 2^L$. The conjugation operation is used to process the chunks if complexity of data chunk is lesser than a predefined threshold α_0[20]. The data chunks which is noise like will be replaced soon by the data chucks $(1-\alpha)$ greater thanα_0, which are noise like image chunks so that they can successfully carry the data. Once the process of data embedding takes place, the image overall is converted back into a system known as PBC. The rate of data embedding of BPCS Steganography can be much more than 4bpp (bit per pixel) without any strong visual artefacts.

4.1.3. Steganography based on noise-adding based

The outcome of concealing data is a couple of value taking place in the Steganography of LSB. In order to get rid of statistical attack on the pair of values, the suggested method is LSB matching in which there are small changes in the techniques of Steganography [21] [22] [23]. The placement of it is made in replacing the cover image's LSB pixels. With the help of LSB matching, the increase or decrease in it takes place by 1 provided that the data bits fail to match these.

The LSB matching indeed is given a special case treatment of $\pm k$ Steganography in the case when $k = 1$ which can higher or lower the pixel values by $\pm k$ for LSB bits matching with that of binary data bit [24]. As a result of $\pm k$ embedding of non adaptive type, there is something the modeling of distortion as an additive independent similar noise signals which are distributed with the PMF (probability mass function) as shown in the following:

$$P_{+k} = \frac{p}{4}, P_0 = 1 - \frac{p}{2}, P_{-k} = \frac{p}{4} \quad (3)$$

N Inside the p equation is the rate of embedding of data in BPP. It was also suggested by Author Fridrich that there is another technique for Noise Adding Steganography known nowadays as Stochastic Modulation [25]. One can hide the data bits inside the cover image which is digital by the addition of a signal of weak noise to a certified but arbitrary probabilistic allocation. In this type of modulation method, the function of parametric parity is utilized. The anti symmetric property is satisfied with the help of it. The parity function suggested by Sharp for x is represented as:

$$Ifx\epsilon[1,2z], p(x,z) = \begin{cases} (-1)^{x+z} & ifz > 0 \\ 0 & ifz = 0 \end{cases} \quad (4)$$

According to the anti symmetric a property $\{Ifx \in [1,2z], p(x,y)\}$is calculated.

For scholastic modulation the procedure of concealing data is visiting the path sequentially or randomly and the stego noise $\xi_n$is incorporated in it, this with a help of a secret key is generated.

From that point, the pixels across the meeting path, one of the specimens of stego noise is rounded off to an integer. As a matter of fact, if the estimation of$z_i = 0$, the pixel $x_i$is then skipped and along with it the next sample n_i for the stego noise $\xi_n$is again rounded and input but at the same time when the value of $z_i \neq 0$there will be alteration in the pixels as per the parity function vales.In the procedure of hiding the data, the out of range pixels [0,255] which are to be truncated surely to the nearest amounts in the range with the required parity. Condition is given below as:

$$Ifp(x_i + z_i, z_i) = m_k theny_i = x_i + z_i$$

$$Elsep(x_i + z_i, z_i) = -m_k theny_i = x_i - z_i$$

Where k^{th} data bit is represented by m_k .The operations regarding the embedding of data in the matching LSB and $\pm k$ Steganography are not alike to that of LSB Steganography. In the stochastic modulation, the data extraction mechanism is to initially generate the sequence z_i of rounded stego noise from the key of stego in a fashion similar to that done while hiding the data. The same path which is pseudo random is followed in the stego image. At the end, the parity function $p(x,z)$ is allowed to the values of pixels.

4.1.4. Steganography based on prediction error

For the maintenance of image's visual quality, to think that secret data must be hidden in a complicated area of image is quite intuitive. The localized level of complexity is estimated to make use of pixel forecast errors. Inside the prediction errors one can hide the data. In order to get the prediction of a present value for pixels the neighboring pixel values can be used to see the differences. It is itself a sort of prediction error. It is an easier way to estimate the errors in prediction. In PVD (pixel value differencing) type of Steganography, an image is assorted into neighboring pixels of the consecutive groups. [26]. Two secret data which are embedded are concealed into the value of differences.

Imagine if the neighborhood pixels p_i and p_{i+1} are there, use the difference $d_i = p_{i+1} - p_i$ in their values where condition is$0 \leq |d_i| \leq 255$.In this case, A large $|d_i|$ indicates a complex block then classify $|d_i|$into a set of contiguous ranges, represented byR_k, where range index is represented by $k = 0,1,2,\ldots,K-1$.Lower bound, upper bound and the width of R_k is represented by l_k, u_k, w_k respectively. w_k is designed to be a power of 2. If $|d_i|\epsilon R_k$then the two pixels corresponding are thought to be carrying $log_2(w_k)$bits, the pixel values of these are changed in such a way that the absolute value of the difference obtained now is equal to$|d_i'| = q_{i+1} - q_i = l_k + v_i$ where $v_i$represents the decimal value is to be inside the embedded bits and procedure is defined as:

$$(q_i, q_{i+1}) = \begin{cases} (p_i - r_c, p_{i+1} + s_f) & if d_i isodd \\ (p_i - r_y, p_{i+1} + s_c) & if d_i iseven \end{cases} \quad (5)$$

Where s_c is represented by $\left\lceil \frac{d_i' - d_i}{2} \right\rceil$and s_f is represented by $\left\lceil \frac{d_i' - d_i}{2} \right\rceil$ in such a way distributing the embedding distortion between two pixels equally. The decimal value inside the embedded bits can be computed by $y_i = |d_i'| - l_k$ but condition is applied where$|d_i'|\epsilon R_k$.

4.1.5. Steganography based on quantization

The quantization index is suggested by Chen and Wornell [27]. QIM is considered as one of the key methodologies uses in the Steganography. The input signals are quantized x into the y (output) with Quantizer set. These are expressed by data bit m. A standard scalar Quantization index modulation with quantization step Δ for embedding binary data is basically defined as:

$$y_i = Q_m(x_i) = \begin{cases} \Delta \left\lfloor \frac{x_i}{\Delta} + \frac{1}{2} \right\rfloor if m_i = 0 \\ \Delta \left\lfloor \left\lfloor \frac{x_i}{\Delta} \right\rfloor + \frac{\Delta}{2} \right\rfloor if m_i = 1 \end{cases} \quad (6)$$

If the QIM standard is added and executed in the spatial domain, $\frac{\Delta}{2} when \Delta > 2$ the sign of discreetness is shown by the histogram inside an integer multiple. It is not much common for a spatial image to have quantization concept. QIM hence is employed frequently to the domain transformation coefficients which are needed to undergo quantization. Noda et al. [28] Highlighted that the with the JPEG compression the QIM can be used. Dither modulation or DM is another name given to irregular QIM. [27] [29].QIM develops the values of output at the points of rebuilding for Quantizer but the dither modulation is likely to generate the signal output and gets all the input value signals. This kind of attained efficiency is done by adding a signal of dither to the input signal before the process of quantization is done and then the deduction of it once after the process of quantization is over. It is depicted as:

$$y_i = Q_m(x_i + d_i) - d_i \quad (7)$$

In the equation mentioned above, a key is used to find out the dither signal and is distributed constantly over$\left[\frac{-\Delta}{2}, \frac{\Delta}{2}\right]$. In the spatial image to bypass the generation of the histogram sparse one can use the dither signal. On the other hand, these are generally used for the transformation of coefficients.

4.2. Frequency domain

Steganography in the picture recurrence area calculations created to expand the execution over their precursors (spatial space techniques). The field of information technology is been increasing rapidly and it is essential to modify the systems of security. With the discovery of data embedding methodology LSB, it is a big milestone in the history of information security. LSB is weekly resistant to attacks and hence the investigators are working on it about the area where they can apply it till they can effectively applied it inside the frequency domain.Two dimensional DCT and its explanation for F (an input image) and T (an output image) is calculated below:

$$T_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} cos \frac{\Pi(2m+1)p}{2m} cos \frac{\Pi(2n+1)q}{2n} \quad (8)$$

Where

$$0 \leq p \leq m-1 \; and \; 0 \leq q \leq 2n-1$$

Also α_p is defined as

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & p = 0 \\ \sqrt{\frac{2}{M}} & 1 \le p \le M-1 \end{cases}$$

$$\alpha_q \text{ is defined as } \alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & q = 0 \\ \sqrt{\frac{2}{N}} & 1 \le q \le N-1 \end{cases}$$

M and N represents the input image dimensions while the variables are m and n and the range of m and n is from 0 $toM-1$ and 0 $toN-1$ respectively. The digital cameras, scanners and other tools used for photography mainly produce JPEG image file format. As a result, secret data hiding in the format of JPEG files can be a much better option. The techniques for Steganography for data embedding to an AC which is alternate current of non zero discrete the transformation cosine in the JPEG image's coefficients, the rate of embedding of data in Steganography is sometimes estimated as per non zero AC DCT per bits coefficient. Discrete cosine transforms (DCT).Each DCT coefficients got from the given equation i.e. equation (8) is supposed to be quantized with an aid of QT, The quantization table. An ultimate aim of this selection with values of this kind is to strictly follow the procedure of experimentation, in that case also a balance is tried to establish among the quality control factors and compression of an operated image. HVS (human visual system) also permits the dictation of certain rations in the quantization table among the values. In order to maintain the data which is quite valuable in descriptors losing up the taut precision at a same time in DCT is considered as a basic aim of quantization.

$$f'(w_x, w_y) = \left\lfloor \frac{f(w_x,w_y)}{r(w_x,w_y)} + \frac{1}{2} \right\rfloor \quad (9)$$

Where

$$(w_x, w_y) \in 0,1, \ldots\ldots\ldots\ldots,7$$

Where
8x8 is the image block is defined by (w_x, w_y)which is overlapping and x is used to mention the coordinates along with y which mentions the function $f'(w_x, w_y)$of results and ⌊ ⌋an operator rounding the floor. In this way we can explain quantization process $r(w_x, w_y)$as:

$$r(w_x, w_y) = \begin{cases} max\left(\left\lfloor \frac{200-2Q}{100} QT(w_x, w_y) + \frac{1}{2} \right\rfloor, 1\right) & 50 \le Q \le 100 \\ \left\lfloor \frac{50}{Q} QT(w_x, w_y) + \frac{1}{2} \right\rfloor & 0 \le Q \le 50 \end{cases} \quad (10)$$

Here, the quality factor is Q and a table for quantization is $QT(w_x, w_y)$. The compression via JPEG later on applies the coding of entropy like Huffman algorithm so as to compress the redundant data $QT(w_x, w_y)$and in this procedure there is a loss of noise, the procedure is therefore called Lossy compression [30]. The scheme mentioned above is a discrete theory which is free of Steganography. As per Li and Wang, the method of Steganography which alters to the $QT$and concealed data is inserted in it in the middle of the coefficients of frequency [31]. The JPEG images are used in these methods for data embedding data. DCT is used in the JPEG compression of images so as to transform the two consecutive sub image blocks into 64 DCT coefficients.

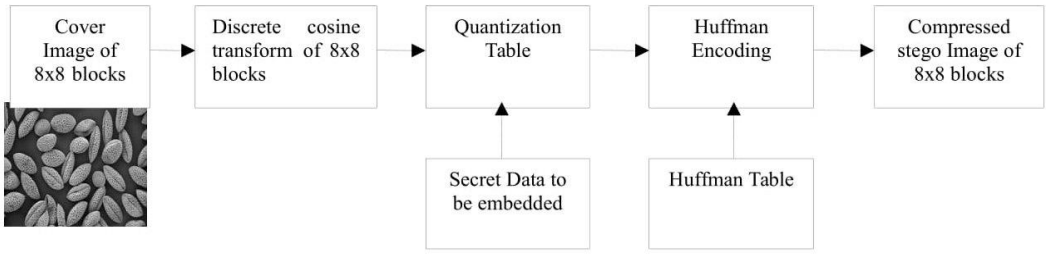


Fig. 4: This Flow Diagram Represents the How to Embed Bits in the Frequency Domain.

The coefficients carry information embedded inside them. On the other hand, the alteration of any of the coefficient will end up in pixels of 64 blocks [32]. As the execution modification of the domain frequency in place of spatial domain, no visual modification is seen in the covered digital image if the provided coefficients are carefully controlled [33].

4.2.1. JSteg algorithm

The initial algorithm to make use of JPEG images is JSteg. The algorithm though stands strong against the visual attacks, it was also established that inspection of the statistical allocation of the coefficients containing DCT shows that data is concealed [34]. The detection of JSteg is simple by the use of$X^2 - test$. Along with that the coefficients of DCT need a careful handling. The JPEG compression coefficients as per Wayner fall along a bell curve and data concealed is embedded by JSteg simply distorts it [35]. Any algorithm making use of PDF function (Probability Density Function) to generate the discriminating characters are fed in a neural network system to detect a data concealed in a domain [36].

Two tools are used for standard JPEG Steganography, JSteg [37] and JPHide [38] making use of a technique of LSB data embedding. The JSteg helps in hiding of the secret data into the cover image by LSB substitution of non-zero DCT quantized coefficients. The DCT quantized coefficients are to be utilized for the concealing of any secret and confidential information bits in the JPHide and these are selected without any aim by a number of generators which are pseudo arbitrary and are not similar to that of JSteg and are controlled by a hidden key. Along with the JPHide, there is also a modifier which alters LSBs of the particular coefficients along with a mode deviation where second minimum bits inside a bit place are supposed to be modified.

4.2.2. F5 steganographic calculation

F5 Steganographic calculations were displayed by Westfeld [39]. It depends on n subtraction and lattice encoding. So it is otherwise called syndrome coding. The outright estimation of the coefficient is diminished by one in the event that it is should have been adjusted as opposed to substituting the LSBs of quantized DCT coefficients with the information bits. Westfeld and Pfitzmann [40], fought that such sort of information installing can't be seen by utilizing the chi-square assault. The calculation F5 inserted information bits into arbitrarily chose DCT coefficients and it likewise utilizes framework installing which limits the vital number of alterations to hide information of certain length. During the time spent information inserting, the length of information and the quantity of non-zero AC coefficients are utilized to decide the best

grid implanting which limits the quantity of alterations of the cover picture.
As per J. Fridrich et.al [41] there is shrinkage when same bit is re-embedded and in case the genuine coefficient is either 1 or -1. In the phase of decoding all the zero coefficients are missed either changed or unchanged. This solid algorithm can be changed with the help of X2- test. Hence for too long, F5 fail to handle the attacks. J.Fridrich et.al [42] also suggested a technique known as Steganalysis to have F5 content detection.

4.2.3. Outguess

N.Provos and P.Honeyman [43] suggested that there is an Outguess in a source code of UNIX. It is much better as a substitute since it is utilized in the generator of pseudo random to find out the coefficients. For Outguess, there are two versions which gained much popularity. OutGuess-0.13b, on which statistical analysis can be conducted while Outguess-0.2 having a potential of conserving the statistical characteristics.
The data embedding procedure in Outguess is carried out in two main phases. In the phase one, the secret data bits in Outguess are embedded along a random walk to the quantized coefficients containing DCT in the LSBs, at the same time 0s and 1s are skipped. At phase 2, correlations are established and coefficients are made which are rejected while the process of embedding takes place and this is to ensure the DCT histogram of the stego image match which folds the image. The Chi square attack cannot be detected by Outguess. [40]. the analysis of X^2-text fails to find any data which has been distributed randomly. Provoset al [43] [44] proposed that with an application of an extended versions of the analysis for X^2-text for the selection of data which is pseudo randomly embedded inside the JPEG images.

4.2.4. YASS steganographic procedure

There is no installment of YASS data in DCT's JPEG coefficients straightforwardly by another procedure of Steganography which is known commonly as YASS. It is somewhat similar to the Steganography of JPEG. [45]. at the place of it a data and a cover image is initially isolated in a spatial portrayal into few of the blocks which are adjusted and maintained at larger and enormous sizes. These are known as well as pieces which are too huge or B squares. 8x8 a further gap is seen between every B square and this is as well alluded to be keeping the host block or H square. The arbitrary selection is made while selecting the hosting squares or blocks with a hidden key so as to carry out the execution of DCT. As a result of it there is an encoding of a confidential information by the help of certain codes which are as well used for the error correction and are installed in the coefficients of DCT of the H obstructs by QIM (Quantization index modulation). The entire picture which is computerized is compact and is passed out as JPEG image once the DCT is executed inverse to the block H. In order of data extraction from stego image, the image is initially decompressed by JPEG into a spatial domain. From DCT coefficients the data is collected from the H blocks. In the end the H blocks position might fail to overlay with the 8x8 JPEG grid. The embedded artifacts for data induced by YASS into the JPEG coefficients of DCT are not directly embedded. One of the strongest techniques is a self calibration in the steganalysis of JPEG for the assessment of statistics inside a cover image. With the help of YASS it is deactivated. [46][47]. There is yet another beneficial outcome of YASS and it is that the data which is embedded might also endure in an active warden scene. The methods like YASS ensure the enhanced security with the help of block randomization suggested by Yu et al [48].Huang et al [49] suggests that a security execution of YASS is comparative and also F5 against other techniques which are state to art and are Steganalytic too.

4.2.5. DWT (discrete wavelet transform)

As we know, Steganography in DWT (discrete wavelet transform), those who are reading generally instructed to keep an eye on some examples which are there already in the literature.[50] [51] [52].Abdulaziz and Pang [53] is of the view that when the quantization vector is used it is said to be LBG (Linde Buzo Gray) which is paired along the block codes commonly called BCH code and 1-stage discrete Haar wavelet transforms. It is also established fact that data transformation with wavelet transform saves some better quality along with the perceptual aretfacts.
Abdelwahab and Hassan [54] suggested that in the domain DWT the technique of Steganography, with the help of DWT the secret and cover images are destroyed. The decomposed images are then divided into discrete disjoint 4×4 blocks and in this way the secret image is blocked and adjusted into the cover blocks so as to find out the ideal pair of it. In the next step, the pair blocks are generated and are inserted into the ideally matched block coefficients in the cover image's HL. For communication, two keys are required, one of it is to hold the indices to the blocks matched in CLL and the other is too matched blocks in the CHL of the cover. It was also suggested by Nag et al that a technique for hiding data is dependent on Huffman coding as well as DWT [55]. Once the Huffman coding is applied and embedded the confidential data in higher frequency parts of the 2-D DWT cover image and low frequency parts are not touched, this is done not to disturb any visual property of an image.

4.2.6. Steganography based on model

Sallee proposed a general structure [56] for the execution of Steganography and the Steganalysis. In this method, the JPEG images will get higher capacity for data and remain secure at a same time from any first order statistical attack. MB needs a career separation into variables of deterministic random X_{det} and indeterministicX_{indet}. A suitable model is needed to have a proper definition of the distribution X_{indet} to resemble the dependencies insideX_{det}. A parameterized model with the definite X_{det} cover image values advance it to a model which is cover specific. The basic cause of this type of model is to find out the distributions which are conditional$P(X_{indet}|X_{det} = X_{det})$. A function of arithmetic decompression is made used for the suitable data which is distributed uniformly in bits for the required distribution ofX_{indet}. This is done by substituting X_{indet} with the similar features and confidential data $X^*{}_{indet}$is added in it.

4.2.7. Adaptive image steganography

The Steganography of an obtained image is a sort of Steganography of an enhanced image. The adaptive Steganography is a case where two older procedures are applied and is also known as statistics aware embedding [3]. "Masking" [34] or model based [56]. The technique needs global statistical features of the image prior to attempting for any interaction with the coefficients of LSB/BCT. It is also dictated by statistics about where the change is to be applied. [57][58]. Pixel's random and adaptive selection depends on the cover image and pixel selection in block with larger and localized STB (standard deviation). The LSB (least significant bit) method of Steganography incorporates the differing of the pixel values (PVD). In this the pixel value difference among the two consecutive pixels is to be estimated and the net secret data bots which are to be embedded into the two pixels. Smooth and edge areas are differentiated with the help of this.
A k-bit LSB substitution technique is needed for the data embedding inside the pixels which are located in the edge areas. Larger payload capacity is the outcome of this method along with premium quality of an image. Another method which is suggested by adaptive image Steganography is the LSB matching which is suggested by A. Ker et al [59]. In this method, the pixels are increased or decreased randomly. J.Spaulding et al proposed BPCS (bit plane complexity segmentation) for the compensation of the discrepancies of the custom LSB procedures of substitution of embedding data. [60]. in a book Wayner describes the noise and calls it "life in noise" also points to how much useful the data embedding is while in noise. It is also proven to be robust in regard to

compression, processing of an image and cropping the image. [32] [61] [62].
Another model based method which is described (MB1) in literature [56], produces an image stego which is based on the model of specified distribution. It results in minimum distortion. Due to the absence of ideal model of Steganography, the algorithmic Steganography can be decomposed with the help of statistics of first order [63]. Furthermore, we can say that it can also be detected how much difference is there between blockiness between an estimated image and a stego based image. [64]. another writer with the discovery of blockiness produced an enhanced version known as MB2, a model which is ideally based on de-blocking.
As per Chin Chen et al. [65], for index based images, the adaptive procedures using the code word classification applied to the procedure of LSB substitution. This is done so as to exploit the actual correlation between surrounding pixels to determine the extent of smoothness and as a result of it the embedding potential was higher too.
Yang et al. [66] narrates that LSB Steganography procedure making use of substitution techniques of PVD, LSB. In this, the pixel difference is used to find out the potential of concealing data into the two pixels. When in the edge areas the pixels located are embedded by a k-bit procedure of LSB substitution, this method is to hide the data which is highly confidential into the edged areas as compared to the smoother areas in the cover image.

5. Analysis

For any image of distortion the measurement of performance is done by with help of $PNSR$ (peak signal to noise ratio) and different metrics are used to classify it on the basis of differences in distortion and are applicable in the images of stego. These are to be defined as:

$$PSNR = 10log_{10}\left(\frac{C^2{}_{max}}{MSE}\right) \tag{11}$$

Where the term MSE represents the Mean Square Error given below:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \tag{12}$$

Where x and y are the coordinates of image, M and N are the dimensions of the image,S_{xy} is the stego-image which is generated and digital cover image is defined as$\mathrm{C_{xy}}$.It ($\mathrm{C^2{}_{max}}$)holds the largest image value.
Where $\mathrm{C^2{}_{max}}$ is defined as:

$$\mathrm{C^2{}_{max}} \leq \begin{cases} 1, \text{double precision} \\ 255, \text{8 bit unit} \end{cases}$$

According to authors [33] [67] [68] [69] for the 8bit grey scale images, the default value $\mathrm{C_{max}} = 255$ can be a case which examines image has 253 fewer representations of grey color. It ($\mathrm{C_{max}}$)is likely to be increased to a power of 2 and as a result intense alteration to PSNR values can be obtained. It ($\mathrm{C_{max}}$)can therefore be defined well as an actual value which is maximum in spite of largest probable value. PSNR is sometimes illustrated at the scale of algorithm in dB, the decibels. Any value of PSNR which is lower than 30dB indicates extremely lower quality and embedding has resulted in this distortion. On the other hand, the stego images of high quality are for more than 40dB.
Van Der Weken et al. [70] suggested identical measures (SMs). The power and efficiency of 10 SMs along with a modified PSNR version is analyzed which was developed on the basis of surrounding chunks having better adaptations to the perception of human beings. Kutter and etitcolas [71] also studied a new measurement which is adapted for the system of human visualizing so as delivering a nice execution and contrast of certain approaches of watermarking in an invisible pattern.

6. Remodeling image steganographic security

There are some of the factors which impact strongly on the security of Steganography such as coefficients and modified pixels, cover image properties, the stego noise signal amplitude etc. in this we have studied some of the techniques for development of Steganography highly robust.

6.1. Improving the data embedding adaptability

It is probably not possible to identify the cover image and stego image if there is no need of cover image to be modified for the passage of information which is to be kept confidential. Hence we can say that security of Steganography and the concerned techniques can be enhanced and when modifications are embedded inside the images, it can decrease the modification probability. Data embedding efficiency is also expressed as the number of bits embedded per one modified embedding. Hence the increase in embedding efficiency is possible. The Steganography and security is improved by it. Crandall [72] proposed and Westfeld [39] helped in the implementation of Matrix encoding procedure where the efficiency of embedding can be increased. The main aim is to keep the coefficients separate into the groups and use the hamming error codes of correction to restrict the each group's modification. A (d; n; k) code is to be modified in most of the coefficients to embed the k bits into the coefficients n. when there is decrease in the rate of embedding, the efficiency of embedding increases and is the main restriction while making use of a hamming code. As per Fridrich et al. [73] Random linear codes can be utilized to cope with the situation when such hate embedding data rate is seen. This is to improve the efficiency of embedding and can be seen inside the articles [74] [75] [76].

6.2. Diminishing the data embedding distortion

With an increase in the efficiency of embedding, it might result in the lessening of embedding modifications for an image. In any case, it can't affirmation that the bending to the picture will diminished.
In the event that all coefficients are not utilized for transmitting information, sender has the opportunity to pick the coefficients which has least resultant modifications after information implanting any deviation. In this way, the stego picture will be excessively near the advanced cover picture factually and perceptually, it enhancing the Steganographic security. In the first place procedure which tending to this issue is perturbed quantization (PQ) steganography [46]. It is comprehended by altering a few coefficients whose quantization mistakes are the base after information installing.

This method can be utilized as a part of an information diminishing procedure that incorporates genuine quantization and change, such as resizing and JPEG. The MME steganography proposed by Kim et al., which adjusting coefficients whose both quantization mistakes and inserting errors are the base while installing information in the duration of the JPEG compression. Uncompressed picture is utilized as info and utilizes network encoding in this procedure all along the information inserting process. Ref. [41] expressed that limiting the implanting distortions makes the steganography less observable. Fridrich talk about that the trade between embedding efficiency and embedding distortion [78].

6.3. Choosing the applicable digital cover image

In some of the conditions, sender has a freedom of selecting the unsuspicious stego images for the secret information transmission. The procedure is suggested by Kharrazi et al. [57] for the selection of the ideal cover images as per the data accessibility of a capable Steganalyser. This also indicates that Steganalyser is not free of errors.

7. Characteristics of steganographic techniques

Features of steganography techniques are given in the Table 1.

Table 1: Important Characteristics of Steganographic Techniques

Steganography	Characteristics
LSB	Least significant modification in a bit
LSB Matching	Random plus or minus 1
Stochastic Modulation	Embedded data noise is modulated
QIM/DM	A data bit is used to determine Quantizer
PVD	(in transform domain generally)
JSteg	Embedding data with the help of pixel difference of the surrounding
MB	JPEG DCT coefficients along with modifications in their least significant bits.
F5	low-precision model to be preserved
YASS	absolute value coefficients are decreased

8. Conclusion

The research in this paper is all about the background of the algorithmic keys for the Steganography of the digital images. Also it has to be kept in mind that several procedures of emerging viz., DCT, DWT and adaptive steganography are not likely to be attacked much easily especially if the data is concealed in smaller size. The main purpose of this is that the coefficients which are modified inside the transformation domain with the help of which image distortion are kept at its minimum value. In special cases these methods try to have below average payload in contrast to the spatial domain algorithms. Bit reduction ways are many in order to encode the data which is hidden. For Steganography the robustness if a tool, since there are so many systems of Steganography which are especially designed to be robust for mapping classes of specified types. It is lucid as well to produce Steganography which isn't easy to be detected and algorithmic Steganography having a potential of resisting the processing of image manipulations which can take place accidentally and not due to any form of attack. This research is also having some recommendations so as to design the Steganography and related systems. The procedures of Steganography are seen struggling to get higher rate of embedding. For channel images, it definitely is a reasonable substitute; there are several outstanding features of the video files to conceal data like good imperceptibility and higher capacity.

References

[1] Hniels Provos & Peter Honeyman,"Hide & Seek: An Introduction to Steganography" IEEE Computer Society Pub-2003.

[2] Ge Huayong, Huang,"Steganography and Steganalysis Based on Digital Image", International conference & signal Processing-2011IEEE.

[3] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2) (1998) 26-34.https://doi.org/10.1109/MC.1998.4655281.

[4] J.C. Judge, Steganography: Past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/stengano graphy/552.php, 2001.

[5] W Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp.313-336, 1996.

[6] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data embedding and watermarking technologies," Proceedings of the IEEE, Vol. 86, No. 6, pp. 1064-1087, June 1998. https://doi.org/10.1109/5.687830.

[7] R. Wolfgang, C. Podilchuk and E. Delp, "Perceptual watermarks for images and video," to appear in the Proceedings of the IEEE, May, 1999. (A copy of this paper is available at: http://www.ece.purdue.edu/~ace).

[8] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, pp. 26-34, February 1998.

[9] R. B. Wolfgang and E. J. Delp, "Fragile watermarking using the VW2D watermark," Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents, SPIE Vol. 3657, San Jose, CA, January 1999.

[10] J. Flores-Escalante, J. Pérez-Díaz and R. Gómez-Cárdenas, Design and Implementation of An Electronic Identification Card, Journal Of Applied Research And Technology.

[11] Aravind K. Mikkilineni, Osman Arslan , Pei-Ju Chiang, Roy M. Kumontoy, Jan P. Allebach,George T.-C.Chiu, Edward J. Delp, Printer Forensics using SVM Techniques , This research was supported by a grant from the National Science Foundation, under Award Number 0219893.

[12] M. Wu, E. Tang, and B. Lin, Data hiding in digital binary image, Proc. of 2000 IEEE International Conference on Multimedia and Expo,vol. 1, pp. 393-396, 2000.

[13] G. Liang, S. Wang, and X. Zhang, Steganography in binary image by checking data-carrying eligibility of boundary pixels, Journal of Shanghai University, vol. 11, no. 3, pp. 272-277, 2007. https://doi.org/10.1007/s11741-007-0317-2.

[14] Jessica Fridrich, Miroslav Goljan, and Rui Du, Reliable detection of lsb steganography in color and Gray scale images. Proc. of 2001 ACM workshop on Multimedia and security: new challenges, pp.27-30, ACM Press, 2001.

[15] P. Alvarez, Using extended file information (EXIF) file headers in digital evidence analysis, International Journal of Digital Evidence, Economic Crime Institute (ECI) 2 (3) (2004) 1–5.

[16] V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011).

[17] Morkel, T., Eloff, J.H.P., Olivier, M.S.: An Overview of Image Steganography. University of Pretoria, South Africa (2002).

[18] Wang, H., Wang, S: Cyber Warfare: Steganography vs. Steganalysis. Communications of the ACM 47(10) (2004). https://doi.org/10.1145/1022594.1022597.

[19] T. Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, June/July 2005.

[20] Eiji Kawaguchi and Richard O. Eason, Principle and applications of bpcs steganography, In Multi-media Systems and Applications, vol. 3528, pp. 464-473, SPIE, 1998.

[21] T. Sharp, An implementation of key-based digital signal steganography, Proc. of the 4th Information Hiding Workshop, vol. 2137, pp. 13-26, Springer, 2001. https://doi.org/10.1007/3-540-45496-9_2.

[22] J. Mielikainen,Lsb matching revisited, IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.https://doi.org/10.1109/LSP.2006.870357.

[23] X. Li, B. Yang, D. Cheng, and T. Zeng, A generalization of lsb matching, IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, 2009. https://doi.org/10.1109/LSP.2008.2008947.

[24] J. Fridrich, D. Soukal, and M. Goljan, Maximum likelihood estimation of secret message length embedded using pmk steganography in spatial domain, Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VII, vol. 5681, pp. 595-606, 2005.

[25] J. Fridrich and M. Goljan, Digital image steganography using stochastic modulation, Proc. Of IST/SPIE Electronic Imaging: Security and Watermarking of Multimedia Contents V, vol. 5020, pp. 191-202, 2003. https://doi.org/10.1117/12.479739.

[26] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value diRerencing, Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626, 2003. https://doi.org/10.1016/S0167-8655(02)00402-6.

[27] B. Chen and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. Information Theory, vol. 47, no. 4, pp. 1423-1443, 2001. https://doi.org/10.1109/18.923725.

[28] H. Noda, M. Niimi, and E. Kawaguchi, High- performance jpeg steganography using quantization index modulation in dct domain, Pattern Recognition Letters, vol. 27, no. 5, pp. 455-461, 2006. https://doi.org/10.1016/j.patrec.2005.09.008.

[29] J.J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, Scalar costa scheme for information embedding, IEEE Trans. Signal Processing, vol. 51, no. 4, pp. 1003-1019, 2003.https://doi.org/10.1109/TSP.2003.809366.

[30] A.C. Popescu, Statistical tools for digital image forensics, Ph.D. Dissertation, Department of Computer Science, Dartmouth College, USA, 2005. Available from:

http://www.cs.dartmouth.edu/~farid/publications/apthesis 05.htmlS, on 16-05-07 at 12:20.
[31] X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007) 3099–31091. https://doi.org/10.1016/j.ins.2007.02.008.
[32] A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, A new genetic algorithm approach for secure JPEG steganography, in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22–23 April 2006, pp. 1–6. https://doi.org/10.1109/ICEIS.2006.1703168.
[33] A.I. Hashad, A.S. Madani, A.E.M.A. Wahdan, A robust steganography technique using discrete cosine transform insertion, in: Proceedings of IEEE/ITI Third International Conference on Information and Communications Technology, Enabling Technologies for the New Knowledge Society, 5–6 December 2005, pp. 255–264.
[34] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Security and Privacy 1 (3) (2003) 32–44. https://doi.org/10.1109/MSECP.2003.1203220.
[35] P. Wayner, Disappearing Cryptography, second ed, Morgan Kaufmann Publishers, 2002.
[36] C. Manikopoulos, S. Yun-Qing, S. Sui, Z. Zheng, N. Zhicheng, Z. Dekun, Detection of block DCT-based steganography in gray-scale images, in: Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9–11 December 2002, pp. 355–358.
[37] Derek Upham, Jsteg, http://zooid.org/ paul/crypto/jsteg/.
[38] Allan Latham, Jphide, http://linux01.gwdg.de/ alatham/stego.html.
[39] A. Westfeld, F5-A steganographic algorithm: high capacity despite better steganalysis, in: Proceedings of Fourth International Workshop on Information Hiding, Lecture Notes in Computer Science, vol. 2137, Pittsburgh, USA, April 2001, pp. 289–302. https://doi.org/10.1007/3-540-45496-9_21.
[40] A. Westfeld and A. Pfitzmann, Attacks on steganographic systems-breaking the steganographic utilities ezstego, JSteg, steganos, and s-tools-and some lessons learned. Proc. Of the 3rd Information Hiding Workshop, vol.1768, pp. 61-76, Springer, 1999. https://doi.org/10.1007/10719724_5.
[41] J. Fridrich, T. Pevny, J. Kodovsky Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities, in: Proceedings of the ACM Ninth Workshop on Multimedia & Security, Dallas, Texas, USA, September 20–21, 2007, pp. 3–14.
[42] J. Fridrich, M. Goljan, D. Hogeg, Steganalysis of JPEG images: breaking the F5 algorithm, in: Proceedings of Information Hiding: Fifth International Workshop, IH 2002 Noordwijkerhout, The Netherlands, Lecture Notes in Computer Science, Springer, October 7–9, 2002, 2578/2003, pp. 310–323.
[43] N. Provos, P. Honeyman, Detecting steganographic content on the Internet, Centre for Information Technology Integration, University of Michigan, Technical report, August 31, 2001.
[44] N. Provos, Defending against statistical steganalysis, Centre for Information Technology Integration, University of Michigan, Technical report, February 2001.
[45] K. Solanki, A. Sarkar, and B. S. Manjunath, Yass: Yet another steganographic scheme that resists blind steganalysis, Proc. of the 9th Information Hiding Workshop, Springer, vol. 4567, pp. 16-31, 2007.https://doi.org/10.1007/978-3-540-77370-2_2.
[46] J. Fridrich, Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes, Proc. of the 6th Information Hiding Workshop, Springer, vol. 3200 , pp. 67-81, 2004. https://doi.org/10.1007/978-3-540-30114-1_6.
[47] Tomas Pevny and Jessica Fridrich, Merging markov and dct features for multi-class jpeg steganalysis. Proc. of SPIE: Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505, pp. 3-14, 2007. https://doi.org/10.1117/12.696774.
[48] Lifang Yu, Yao Zhao, Rongrong Ni, and Yun Q. Shi, A high-performance yass-like scheme using randomized big-blocks, Proc. of the IEEE International Conference on Multimedia and Expo (ICME 2010), 2010.
[49] Fangjun Huang, Jiwu Huang, and Yun Qing Shi, An experimental study on the security performance of YASS, IEEE Trans. Information Forensics and Security, vol. 5, no. 3, pp. 374-380, 2010. https://doi.org/10.1109/TIFS.2010.2054082.
[50] W.Y. Chen, Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation, Applied Mathematics and Computation 185 (1) (2007) 432–448. https://doi.org/10.1016/j.amc.2006.07.041.
[51] V.M. Potdar, S. Han, E. Chang, A survey of digital image watermarking techniques, in: Proceedings of the IEEE Third International Conference on Industrial Informatics (INDIN), Perth, Australia, 10–12 August 2005, pp. 709–716.
[52] B. Verma, S. Jain, D.P. Agarwal, Watermarking image databases: a review, in: Proceedings of the International Conference on Cognition and Recognition, Mandya, Karnataka, India, 22–23 December 2005, pp. 171–179.
[53] N.K. Abdulaziz, K.K. Pang, Robust data hiding for images, in: Proceedings of IEEE International Conference on Communication Technology, WCC- ICCT'02, vol. 1, 21–25 August 2000, pp. 380–383. https://doi.org/10.1109/ICCT.2000.889233.
[54] A.A. Abdelwahab, L.A. Hassan, A discrete wavelet transform based technique for image data hiding, in: Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, March 18–20, 2008, pp. 1–9.https://doi.org/10.1109/NRSC.2008.4542319.
[55] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, A novel technique for image steganographybased on DWT and Huffman coding, IJCSS, vol. 4, no. 6, pp. 561-570.
[56] P. Sallee, Model-based steganography, Proc. of the 2nd International Workshop on Digital Water-marking, vol. 2939, pp. 154-167, Springer, 2003.
[57] M. Kharrazi, H.T. Sencar, N. Memon, Performance study of common image steganography and steganalysis techniques, Journal of Electrical Imaging 15 (4) (2006) 1–16.
[58] R. Tzschoppe, R. Baum, J. Huber, A. Kaup, Steganographic system based on higher-order statistics, in: Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. Santa Clara, California, USA 2003, vol. 5020, pp. 156–166. https://doi.org/10.1117/12.477301.
[59] A. Ker, "Steganalysis of LSB Matching in Grayscale Images." IEEE Signal Processing Letters, vol. 12(6), pp. 441–444, 2005 https://doi.org/10.1109/LSP.2005.847889.
[60] J. Spaulding, H. Noda, M.N. Shirazi, E. Kawaguchi, BPCS steganography using EZW lossy compressed images, Pattern Recognition Letters 23 (13) (2002) 1579–1587. https://doi.org/10.1016/S0167-8655(02)00122-8.
[61] C.C. Chang, H.W. Tseng, A steganographic method for digital images using side match, Pattern Recognition Letters 25 (12) (2004) 1431–1437. https://doi.org/10.1016/j.patrec.2004.05.006.
[62] E. Franz, A. Schneidewind, Adaptive steganography based on dithering, in: Proceedings of the ACM Workshop on Multimedia and Security, September 20– 21, 2004, Magdeburg, Germany, pp. 56–62. https://doi.org/10.1145/1022431.1022443.
[63] R. Bohme, A. Westfeld, Breaking cauchy model-based JPEG steganography with first order statistics, in: Proceedings of the European Symposium on Research in Computer Security, ESORICS 2004, Valbonne, France, 13th September 2004, Lecture Notes in Computer Science, vol. 3193, p p. 125–140. https://doi.org/10.1007/978-3-540-30108-0_8.
[64] L. Yu, Y. Zhao, R. Ni, Z. Zhu, PM1 steganography in JPEG images using genetic algorithm, Soft Computing 13 (4) (2009) 393–400. https://doi.org/10.1007/s00500-008-0327-7.
[65] C.C. Chang, P. Tsai, M.H. Lin, An adaptive steganography for index- based images using code word grouping, Advances in MultimediaInformation Processing-PCM, Springer, vol. 3333, 2004, pp. 731– 738.
[66] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun Adaptive data hiding in edge areas of images with spatial LSB do-main systems. IEEE Transactions on Information Forensics and Security, 2008, vol. 3, no. 3, p. 488-497. https://doi.org/10.1109/TIFS.2008.926097.
[67] Y.H. Yu, C.C. Chang, I.C. Lin, A new steganographic method for color and grayscale image hiding, Computer Vision and Image Under-standing 107 (3) (2007) 183– 194. https://doi.org/10.1016/j.cviu.2006.11.002.
[68] M. Drew, S. Bergner, Spatio-chromatic de-correlation for color image compression, Technical Report, School of Computing Science, Simon Fraser University, Vancouver, Canada, 2007, available from:/http:// fas.sfu.ca/pub/cs/TR/2007/CMPT2007-09.pdfS.
[69] M. Saenz, R. Oktem, K. Egiazarian, E. Delp, Colour image wavelet compression using vector morphology, in: Proceedings of the European Signal Processing Conference, September 5–8 2000, Tampere, Finland, 2000, pp. 5–8.
[70] D. Van Der Weken, M. Nachtegael, E. Kerre, Using similarity measuresand homogeneity for the comparison of images, Image and Vision Computing 22 (9) (2004) 695–702. https://doi.org/10.1016/j.imavis.2004.03.002.
[71] M. Kutter, F. Petitcolas, A fair benchmark for image watermarking systems, in: Proceedings of Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, California, USA, 25–27 January 1999, vol. 3657, pp. 226–239.

[72] R. Crandall, Some notes on steganography, Posted on steganography mailing list, http://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998.
[73] J. Fridrich and D. Soukal, Matrix embedding for large payloads, IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 390-395, 2006. https://doi.org/10.1109/TIFS.2006.879281.
[74] W. M. Zhang, X. P. Zhang, and S. Z. Wang, A double layered plus-minus one data embedding scheme, IEEE Signal Processing Letters, vol. 14, no. 11, pp. 848-851, 2007. https://doi.org/10.1109/LSP.2007.903255.
[75] J. Fridrich, P. Lisonek, and D. Soukal, On steganographic embedding efficiency, Proc. of the 8th Information Hiding Workshop, Springer, no. 4437, pp. 282-296, 2007.
[76] JAurgen Bierbrauer and Jessica Fridrich, Constructing good covering codes for applications in steganography, LNCS Trans. Data Hiding and Multimedia Security III, vol. 4920, pp. 1-22, 2008. https://doi.org/10.1007/978-3-540-69019-1_1.
[77] Y. Kim, Z. Duric, and D. Richards, Modified matrix encoding for minimal distortion steganography. Proc. of the 8th Information Hiding Workshop, Springer, vol. 4437, pp. 314-327, 2006.
[78] Jessica Fridrich, Minimizing the embedding impact in steganography, Proc. of the 8th ACM workshop on Multimedia and Security, ACM Press, pp. 2-10, 2006.