International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 1 Issue: 10 782 – 792

Data Hiding in Gray-Scale Images by LSB Method using IWT with Lifting Scheme

Urmila Kumari
M.Tech.*(RTU, Kota)
Dept of Computer Science & Engineering
Sri Balaji College of Engineering & Technology
Jaipur, Rajasthan (India)
silayach.urmila@gmail.com

Saroj Hiranwal
Reader
Dept of Computer Science & Engineering
Sri Balaji College of Engineering & Technology
Jaipur, Rajasthan (India)
ersaroj_hiranwal@rediffmail.com

***Abstract* — This paper introduced a completely unique steganography technique to extend the capability and therefore the physical property of the image once embedding. Genetic rule utilized to get associate degree optimum mapping operate to minimize the error distinction between the quilt and therefore the stego image and use the block mapping technique to preserve the native image properties. Additionally we have a tendency to applied the OPAP to extend the activity capability of the rule compared to different systems. However, the process complexness of the new rule is high. The simulation results showed that capability and physical property of image had enlarged timing. Also, we will choose the most effective block size to scale back the computation value and to extend the PSNR victimisation optimisation algorithms like GA.**

Keywords- *Steganography, Message Embedding, LSB, Optimal Pixel Adjustment process, SNR, PSNR.*

*****

I. INTRODUCTION

Since the increase of the web one in every of the foremost vital factors of knowledge technology and communication has been the protection of knowledge. Cryptography was created as a method for securing the secrecy of communication and plenty of totally different strategies are developed to inscribe and decipher information so as to stay the message secret. sadly it's typically not enough to stay the contents of a message secret, it's going to even be necessary to stay the existence of the message secret. The technique accustomed implement this, is named steganography.

Steganography is that the follow of activity non-public or sensitive data at intervals one thing that seems to be nothing out of the standard. Steganography is commonly confused with science as a result of the 2 are similar within the means that they each are accustomed shield vital data. The distinction between the 2 is that Steganography involves activity data therefore it seems that no data is hidden in the least. If an individual or persons views the article that is hidden inside he or she's going to don't have any concept there's any hidden information, thus the person won't conceive to decipher the data.

Steganography comes from the Greek words Steganos (Covered) and Graptos (Writing). Steganography within the modern-day sense of the word typically refers to data or a file that has been hid within a digital image, Video or Audio file. What Steganography basically will is exploit human perception, human senses aren't trained to appear for files that have data hidden inside them, though there are programs obtainable which will do what's referred to as Steganalysis (Detecting use of Steganography). the foremost common use of Steganography is to cover a file within another file. Once data or a file is hidden within a carrier file, the info is sometimes encrypted with a word.

Steganography nowadays, however, is considerably a lot of refined than the examples higher than counsel, permitting a user to cover massive amounts of knowledge at intervals image and audio files. These varieties of steganography typically are employed in conjunction with cryptography in order that the data is doubly protected; initial it's encrypted so hidden in order that associate degree oppose must initial notice the data (an typically troublesome task in and of itself) so decipher it.

There are variety of uses for steganography besides the mere novelty. One in every of the foremost wide used applications is for alleged digital watermarking. A watermark, traditionally, is that the replication of a picture, logo, or text on paper stock in order that the supply of the document may be a minimum of partly attested. A digital watermark will accomplish constant function; a printmaker, as an example, would possibly post sample pictures on her information processing system complete with associate degree embedded signature in order that she will be able to later prove her possession just in case others conceive to portray her work as their own. It also can be accustomed permit communication at intervals associate degree underground community. There are many reports, as an example, of persecuted spiritual minorities victimization steganography to engraft messages for the cluster at intervals pictures that are denote to illustrious internet sites.

II. RELATED WORK

Many different steganographic schemes are come back up with for varied types of pictures. We will classify the

prevailing schemes in step with the format of the quilt image as follows: Steganography for grayscale images/spatial domain [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]: These schemes usually directly insert a little piece of the key message into the least-significant-bit of every image pixel within the abstraction domain. There are some benefits to victimization the abstraction domain to cover data: (1) it's less complicated and quicker to implement the technique; (2) it will a lot of simply supply a high activity capacity; (3) the stego-image quality may be a lot of simply controlled. As a result, the grayscale image has become a preferred reasonably image once it involves secret information activity. As a matter of truth, we will more classify these grayscale image steganographic schemes into 2 types: (1) high activity capability strategies [7, 8, 13]: schemes whose embedding algorithms operate in a very pixel-by-pixel manner, leading to the activity capability of [*fr1] the quilt image size, taking no human visual sensitivity into thought with a simply acceptable stego-image quality, and (2) high physical property strategies [3, 9, 12]: schemes whose embedding algorithms are human-visual-sensitivity-related, leading to a distinct payload worth for every individual pixel. The latter kind tends to preserve a lot of image details, giving the next degree of imperceptibility; but, this can be done at the sacrifice of the activity capability.

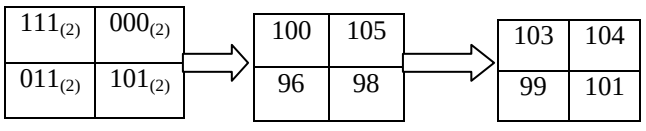
Steganography for JPEG images/frequency domain [14, 15, 16, 17]: The JPEG image is presently the foremost common compression file format obtainable on the web. Therefore, it's a lot of convenient to use JPEG pictures to convey secret information than grayscale pictures. However, the image distortion is sometimes terribly serious once the DCT coefficients are changed for the activity of the key information, and thus the poorly restricted, hardly increasable activity capability may be a major drawback.
Steganography for binary pictures [18, 19, 20, 21]: it's additionally more difficult to cover secret information in binary pictures as a result of there are solely 2 alternatives to the colour of a binary image. The modifications done to the image attributable to the embedding of the key information may be simply discernible by the human eye, which provides a strict limit to the activity capability of the binary image compared with the grayscale image. Among the presently obtainable steganographic techniques for binary image, Shanghai dialect and Liu's technique [21] may be a excellent alternative if the standard of the stego-image is that the major concern. However, the hidden capability is on prime of the priority list, then Tseng et al.'s [18] technique is that the most extremely suggested.
Steganography for palette pictures (i.e., Gif images) [22, 23, 24]: Palette pictures, rather like JPEG pictures, are wide used over the web. Palette pictures are composed of a color palette and a few image information (i.e., index data). once embedding secret information, if it's the colour palette that's changed, then major distortions will occur even once solely a small part of the colour palette is altered. that's to mention, modifying the image information would be the higher alternative if the stego-image quality is that the major concern. However, whether or not the key message is embedded on the colour palette aspect or the image information aspect, palette image steganographic schemes don't appear terribly probably to be capable of providing a high payload.
In this paper, we have a tendency to shall focus solely on grayscale image steganography. the remainder of this paper is organized as follows. In Section two, we have a tendency to shall introduce some connected works, as well as high activity capability strategies [7] and high stego image quality schemes [9, 12]. Then, in Section three, we have a tendency to shall consistently compare and analyze the schemes introduced in Section two, in order that we will come back to some crucial, constructive ideas, which can function our directions for future analysis mentioned in Section four, followed by a quick conclusion given in Section five.

Steganography for Grayscale Picture

In this section, we have a tendency to shall introduce many strategies that hide secret information within the abstraction domain. In general, a grayscale image pixel worth includes eight bits, and therefore the last 3 bits of every pixel may be accustomed hide secret information while not inflicting any distortion that's perceptible to the human eye. For this reason, grayscale pictures are wide used for activity information owing to their larger activity capacities over different image formats. one in every of the foremost noted techniques during this class is that the LSBs (Least-Significant-Bits) technique, that directly embeds the key information into the smallest amount important bits of the pixel worth. The earliest rule is named the easy LSBs technique, and its embedding rule is as follows.

Steganography by the easy LSBs Method

Suppose Pi is a few pixel worth of a picture. The pixel worth of Pi, expressed in its binary type, is as follows:
$Pi = (b_7b_6b_5b_4b_3b_2b_1b_0)_2 = \text{Sum of n 0 to 7 } b_n \times 2_n$ Where b7 is the most significant bit and b0 is the least significant bit. Usually, the last 3 bits b2, b1 and b0 may be accustomed hide secret information, which is what we have a tendency to decision the 3-LSBs theme. The stego-image quality the 3-LSBs theme can give is just acceptable. The embedding procedure of the easy LSBs theme runs in a very pixel-by-pixel fashion; particularly, the payload of every pixel is identical. Assume the task here is to cover these 3 bits of secret information (s2s1s0)(2) into Pi; in different words, the 3 bits (s2s1s0)(2) are to be inserted into the last 3 bits b2b1b0.



Secret Message Cover Image Stego Image

Fig. 1 Simple 3-LSBs method

Fig. 1 is associate degree illustration showing however the 3-LSBs theme will have the task done. As Fig. 1 suggests, every pixel of the quilt image finishes up holding three bits

of secret information. the primary pixel worth is Pi=100(10), and its binary worth is 01100100(2). we will directly insert 3 bits of secret information 111(2) into its last 3 bits 100(2). This way, the binary worth 01100100(2) is currently turned into 01100111(2), and therefore the stego-image Pi'=103 may be obtained by reworking 01100111(2) into its decimal worth.

Steganography by the Optimum LSBs Method

The simple LSBs technique may be changed in order that the stego-image quality gets improved [7, 8, 13]. The embedding algorithms of such improved schemes are still supported that of the easy LSBs technique. during this section, we have a tendency to introduce one in every of the improved strategies referred to as the optimum LSBs technique [1]. The theme will greatly improve the stego-image quality by applying associate degree optimum pixel adjustment method. In Ref. [1], 3 candidates are picked out from the pixels and compared to examine that one can have the most effective result (closest to the initial pixel value) with the key information embedded in. the most effective candidate is then referred to as the optimum pixel and is employed to hide the key information.

Steganography by the PVD technique

In 2003, Shanghai dialect associate degreed Tsai [9] conferred an adaptive steganographic theme supported pixel-value differencing (PVD). With their technique, the payload of every individual pixel may be totally different, and therefore the resultant stego-image quality is very fine with excellent modification invisibleness. The activity capability varies between smooth areas and edge areas, enabling edge areas to carry a lot of secret information than swish areas. this can be as a result of the degree of distortion tolerance of a position space is of course more than that of a swish space. additionally, the options of the image blocks keep unchanged once Shanghai dialect and Tsai's theme is applied, which means that the embedding of the key information doesn't modification any swish space into a position space or any edge space into a swish space. Therefore, the stego-image quality the PVD technique produces is best than what different LSBs-based strategies can give in terms of human beholding.

Steganography by the MBNS technique

In 2005, Zhang associate degreed Wang [12] additionally conferred an adaptive steganographic theme with the multiple-base writing (MBNS) supported human vision sensitivity (HVS). The activity capability of every image pixel is decided by its alleged native variation. The formula for computing the native variation takes under consideration the issue of human visual sensitivity. a good native variation worth indicates the actual fact that {the space| the world| the realm} wherever the pixel belongs may be a busy/edge area, which suggests a lot of secret information may be hidden. On the contrary, once the native variation worth is little, less secret information are hidden into the image block as a result of it's in a very swish space. This way, the stego-image quality degradation is incredibly invisible to the human eye.

Comparisons and Analyses

In this section, we have a tendency to shall initial compare performances of the easy LSBs technique and therefore the optimum LSBs technique in terms of stego-image quality, so we have a tendency to shall analyze the acacias of the PVD technique and therefore the MBNS technique. to start with, some experimental results are given to demonstrate that the optimum LSBs technique will greatly improve the stego-image quality provided by the easy LSBs technique. The PSNR worth of the optimum LSBs theme is larger than that of the easy LSBs technique by concerning two.22»3.03 dB. Please pay special attention to the actual fact that the stego image quality of 4-LSBs by victimization the optimum theme remains acceptable to the human eye. However, the PSNR worth drops sharply all the way down to twenty eight dB even once 5-LSBs is employed to engraft secret information. Moreover, the embedding result within the smooth areas is conspicuous to the attention once the 4-LSBs theme is employed. However, the optimum LSBs technique will still meet the high activity capability demand as a result of no top quality theme [3, 9, 12] will conceal information over [*fr1] the scale of the quilt image. Therefore, the optimum LSBs technique may be a a lot of ideal theme once a high payload is needed. against this, the PVD technique and therefore the MBNS technique are a lot of appropriate for low activity capability applications as a result of they are higher at conserving image details once the embedding of the key information. Suppose there are 2 consecutive pixels from a swish space. the 2 swish space pixels can stay swish once the process of the PVD technique, whereas the property of the 2 pixels would possibly modification if it's a LSBs based mostly theme that's accustomed hide the key information. From the point of view of human vision sensitivity, the MBNS theme is best than the PVD theme, and therefore the reason is that the previous has a lot of parameters than the latter. within the MBNS theme, the native variation of every pixel is decided by 3 close pixels, whereas the PVD theme refers to solely 2. Therefore, with the MBNS technique, the image native property may be a lot of objectively and exactly measured.

Directions for Future analysis

Our future analysis efforts are targeted on creating a replacement technique that includes a larger activity capability than the 4-LSBs technique and might maintain such stego-image quality on meet the demand of human visual sensitivity. the subsequent are some directions for future research:

(1) Make higher use of edge areas to cover a lot of information: If five bits of secret data were to be hidden in each pixel, so the visual artifacts on the stego-image would be clearly visible. that's to mention, not each pixel will afford to carry such a large amount of secret information bits while not clearly showing the modification. In our opinion, the full image ought to a minimum of be de-escalated to swish areas and edge areas, and information activity will

then be done to totally different types of areas otherwise. In swish areas, as an example, we will hide four bits of secret information in every pixel; in edge areas, every pixel will afford to carry as several as five bits of secret information. However, it's necessary however more difficult to do to keep up the native properties of the pixels, creating them keep constant once activity information, because, say, if some swish space is modified into a non-smooth space once activity information, it'll end in decision making errors within the recovery section. Therefore, the extracting rule should be blind.

(2) Utilize a lot of close pixels to see the native complexness of the image pixel: In Shanghai dialect and Tsai's technique [9], the native characteristics of the image is decided by 2 pixels. In Zhang and Wang's technique [12], the native variation of every pixel depends on its 3 close pixels. In our opinion, at intervals an inexpensive limit, a lot of close pixels mean a lot of correct native variation. for example, we will cipher the native variation supported a three £ three sub-block style. all the same, if the quantity of close pixels picked bent verify the native variation gets too huge, the sub-block loses its sense of neighborhood, and therefore the native variation derived can build very little sense if any. In different words, {the drawback |the matter} of what {number} pixels build the right number to require under consideration once we cipher the native variation may be a major problem to resolve within the future.

(3) In recent years, several steganalysis schemes are planned with the thought of police work the existence of the hidden information within the stego-image by victimization data point steganalysis attacks [25, 26, 27, 28, 29]. Indeed, it's a lot of economical and correct to gauge whether or not there's any secret message hidden in a very digital image by victimization steganalysis than by simply gazing the image. To deal with this new trend, new steganographic techniques that we have a tendency to are reaching to develop within the future ought to be powerful enough to face up to the attacks of steganalysis detection.

III. PLANNED SYSTEM

Embedding Method

The Embedding Algorithm: The blocks of the embedding rule are explained within the following steps:

Step 1: scan the hide image file into a 2 dimensional decimal arrays.

Step 2:Histogram modification forestall overflow/underflow that happens once the modified values in whole number moving ridge coefficients manufacture stego image pixel values to exceed 255 or to be smaller than zero. This drawback was found to be caused by the values close to 255 or zero.

Step 3: Divide the hide image into 8x8 non overlapping blocks. By this division every 8x8 block may be categorized as a swish or advanced block.

Step 4: Remodel every block to the remodel domain victimization Haar whole number moving ridge remodel ensuing LLI, LHI, HLI and HHI.

Step 5: Verify the activity capability of every coefficient; we have a tendency to use a changed version of the activity capability operate. From experiments we have a tendency to found that as we have a tendency to lower the bits accustomed hide the key message within the LL sub band the resulted distortion within the stego-image becomes smaller; in order that we have a tendency to changed this activity capability operate by victimization totally different ranges for k for the ICSH, hectoliter and HH sub bands wherever its values are type one to four. For the LL sub band the worth of k is up to zero and in some cases the bits used is fastened to solely bits to boost the stego-image quality.

Step 6: Engraft L bits of message into the corresponding haphazardly chosen coefficients. Random choice of coefficients provides security wherever the sequence of the message is merely illustrious to each sender and receiver by employing a antecedently prearranged secret key.

Step 7: Apply optimum pixel adjustment rule, once taking into thought {that every} changed constant stays in its activity capability vary wherever each worth of L is verify in step with absolutely the worth of the moving ridge coefficients any important modification during this worth can manufacture totally different worth of L to be calculated at the receiver. The good plan of victimization the optimum pixel adjustment (OPA) rule is to scale back the error distinction.

Cryptography is that the science of encrypting information in such some way that nobody will perceive the encrypted data, whereas in Steganography the existence of information is formed means that its presence can't be viewed. The data to be hidden is embedded into the quilt object which might be text, image, audio or video in order that the looks of canopy object doesn't vary even once the data is hidden. To use a lot of security the info to be hidden is encrypted with a key before embedding. To extract the hidden message one ought to have the key. A stego object is one, that appearance specifically same as cowl object with associate degree hidden message. Secure secret communications wherever cryptological secret writing strategies aren't obtainable. Secure secret communication wherever robust cryptography isn't potential. The military aspect communication may be terribly importance in security purpose between the initial constant worth and therefore the altered worth by checking the correct next bit to the changed LSBs in order that the resulted modification are negligible.

For example, if a binary range one thousand (decimal range 8) is modified to 1111 (decimal range 15) as a result of 3 LSB's were replaced with embedded data; the distinction from the initial range is seven. This distinction within the original worth is outlined as associate degree embedding error. By adjusting the fourth bit from a worth of I to a worth of zero, the binary range becomes 0111 (decimal range 7) and therefore the embedding error is reduced to I whereas at constant time protective the worth of the 3 embedded bits. The ultimate step within the planned technique, wherever it will scale back the error by [*fr1]. the good plan of OPA is to see the bit right next to the last modified LSBs is employed to scale back the error resulted once insertion of message bits.

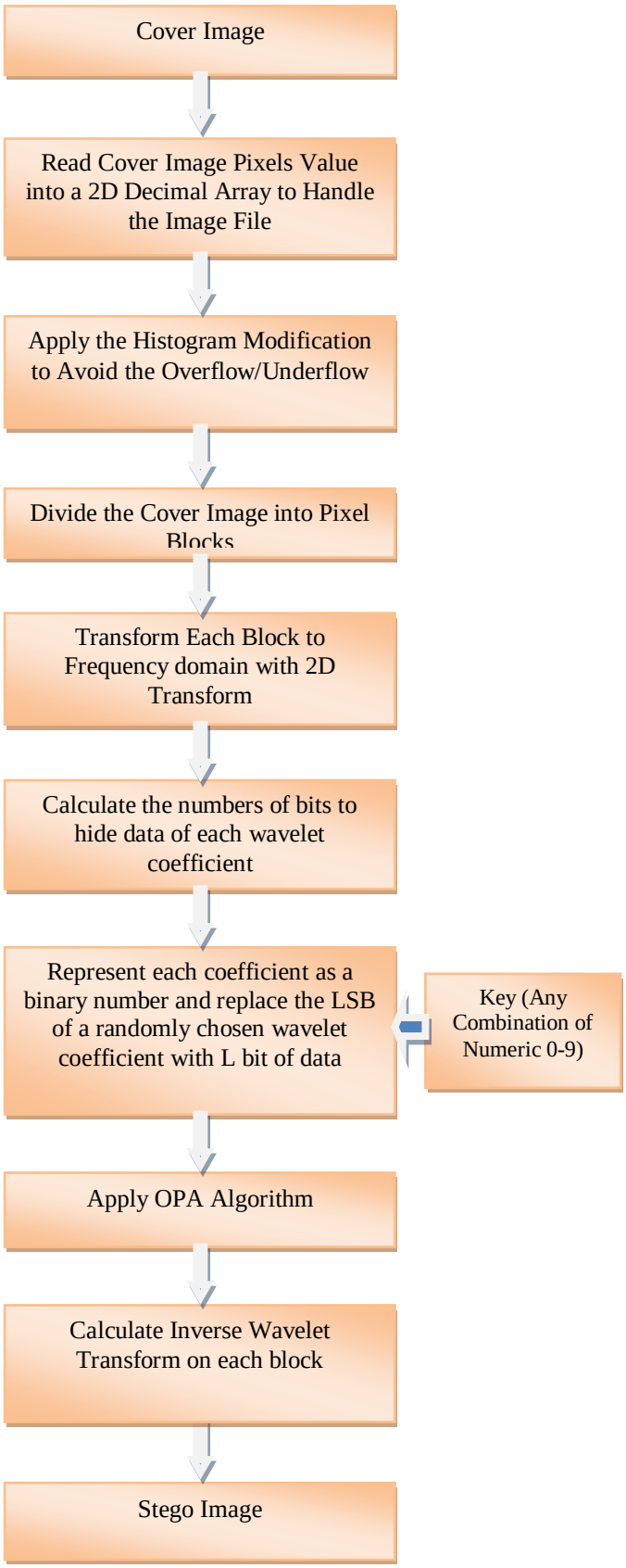


Fig. 2 Block diagram of Embedding algorithm

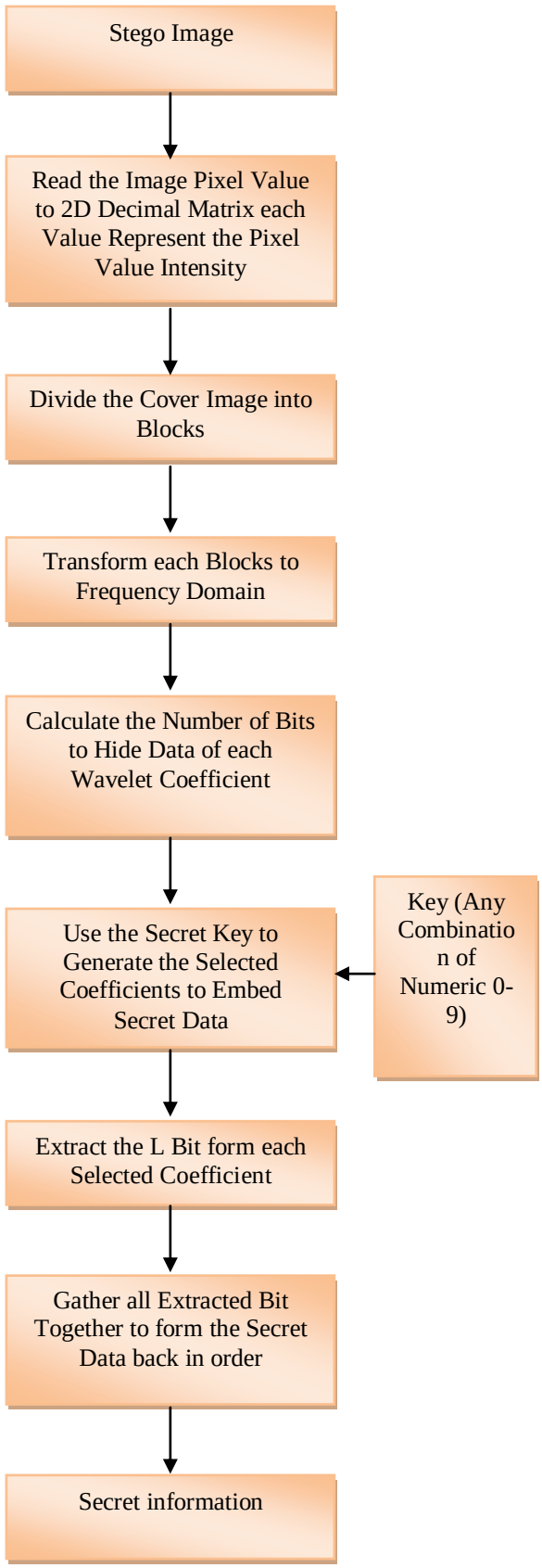


Fig. 3 Block diagram of Extraction algorithm

Step 8: Finally, verify the inverse whole number moving ridge remodel on every 8x8 block to revive the image to abstraction domain.

The main plan of victimization the optimum pixel adjustment (OPA) rule is to scale back the error distinction between the initial constant worth and therefore the altered worth by checking the correct next bit to the changed LSBs in order that the resulted modification are negligible.

The rule is that the final step within the planned technique, wherever it will scale back the error by [*fr1]. The most plan of OPA is check the bit right next to the last modified LSBs is employed to scale back the error resulted once insertion of message bits.

Extraction method

MATLAB may be a numerical computing atmosphere and fourth-generation artificial language. Created by mathematics Works, MATLAB permits matrix manipulations, plotting of functions and information, implementation of algorithms, creation of user interfaces, and interfacing with programs written in different languages, as well as C, C++, Java, and algebraic language.

Although MATLAB is meant primarily for numerical computing, associate degree elective chest uses the MuPAD symbolic engine, permitting access to symbolic computing capabilities. a further package, Simulink, adds graphical multi-domain simulation and Model-Based style for dynamic and embedded systems. At the receiver uses the extraction rule to get the key data. The diagram of the extraction rule is shown in fig. 3

I. EXPERIMENTAL RESULTS

The planned implementation of RS-analysis victimization genetic rule for the sturdy security in Steganography application is finished on customary 32-bit windows OS with one.84 rate processor and a couple of GB RAM. The planned technique is applied on 512x512 8-bit grayscale pictures “Jet”, “Boat”, “Baboon” and “Lena”. The messages are generated haphazardly with constant length because the most activity capability.

Fig. 4 Cover Images

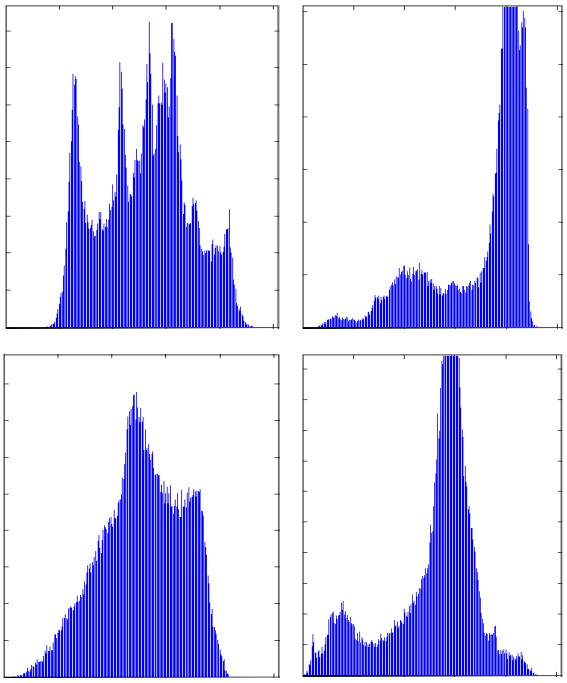


Fig. 5 Four Gray Scale Image Histogram

The table one and a couple of are shown varied values like the values of R_m-R_{-m} and S_m-S_{-m} that represents the RS-steganalysis on regular and singular block. It may be simply seen that {the worth} of R_m-R_{-m} and S_m-S_{-m} will increase from initial value before embedding and once embedding that exhibits a powerful correlation in potential of RS-analysis and designed module. At initial stage the values are less, once embedding the message, values will increase and at last once applying optimum pixel adjustment method values are decreases. Human sensory system is not able to differentiate the coloured pictures with PSNR over thirty six dB. This planned work embedded the messages within the k-LSBs, from k=3 to k=5 and received an inexpensive PSNR. Table three presents the results and it show that for k up to four, we've got the best capability of information activity and affordable visual quality. The planned work embedded the message within the three, 4-LSBs and received a high PSNR. So, we have a tendency to take k worth up to four because the range of bits per pixel. we will increase the capability up to 5-LSBs. Table three shows the capability and therefore the PSNR of the planned technique for 3-LSBs.

Figure five shows the photographs once embedding 3-LSBs and 4-LSBs. As we have a tendency to compare these embedded pictures with the input cowl pictures as shown in figure four, we have a tendency to notice that there aren't any important changes in pictures. The embedded pictures appears like as same as cowl pictures. That the attackers don't notice in between communication of 2 parties that secret message embedded in these pictures.

Table four shows the results of embedding capability, varied issue values and PSNR values for 10 gray and coloured pictures. Figure five shows that pictures for k up to four that there's no important modification within the stego-image

bare graph for 4-LSBs pictures, so it's secured against any data point attack.

TABLE 1 DIFFERENT VALUES FOR GRAY SCALED IMAGES (K=3)

IMAGE NAME	R_m-R_{-m} VALUES			S_m-S_{-m} VALUES		
	STARTING VALUE	AFTER PROCESS	After ADJUSTMENT	STARTING VALUE	AFTER PROCESS	After ADJUSTMENT
LENA	0.0029494	0.40787	0.37519	0.0059184	0.40966	0.37007
JET	0.0082034	0.40787	0.37482	0.00041727	0.40966	0.037132
BABOON	0.0089319	0.40787	0.37783	0.0043593	0.40966	0.37009
BOAT	0.0080646	0.40787	0.3707	0.00074112	0.40966	0.36869

TABLE 2 DIFFERENT VALUES FOR GRAY SCALED IMAGES (K=4)

IMAGE NAME	R_m-R_{-m} VALUES			S_m-S_{-m} VALUES		
	STARTING VALUE	AFTER PROCESS	After ADJUSTMENT	STARTING VALUE	AFTER PROCESS	After ADJUSTMENT
LENA	0.0084982	0.10401	0.076644	0.0050063	0.10991	0.072923
JET	0.00069687	0.10401	0.078048	0.0020586	0.10991	0.069175
BABOON	0.0069136	0.10401	0.074958	0.069931	0.10991	0.072535
BOAT	0.004499	0.10401	0.072014	0.0013425	0.10991	0.072022

Table 3 Image size, Embedding size in bits and PSNR Values (K=3)

Cover Image	Type of Image	Size of Image	Embedding Bits	Size of Data	PSNR(db)
Lena	Gray Scale	38.7 KB	534344	65.2 KB	54.83
Jet	Gray Scale	58.4 KB	534344	65.2 KB	33.51
Baboon	Gray Scale	112 KB	534344	65.2 KB	57.83
Boat	Gray Scale	36.1 KB	534344	65.2 KB	54.83

Table 4 Image size, Embedding size in bits and PSNR Values (K=4)

Cover Image	Type of Image	Size of Image	Embedding Bits	Size of Data	PSNR(db)
Lena	Gray Scale	38.7 KB	2137696	65.2 KB	54.83
Jet	Gray Scale	58.4 KB	2137696	65.2 KB	33.51
Baboon	Gray Scale	112 KB	2137696	65.2 KB	57.83
Boat	Gray Scale	36.1 KB	2137696	65.2 KB	54.83

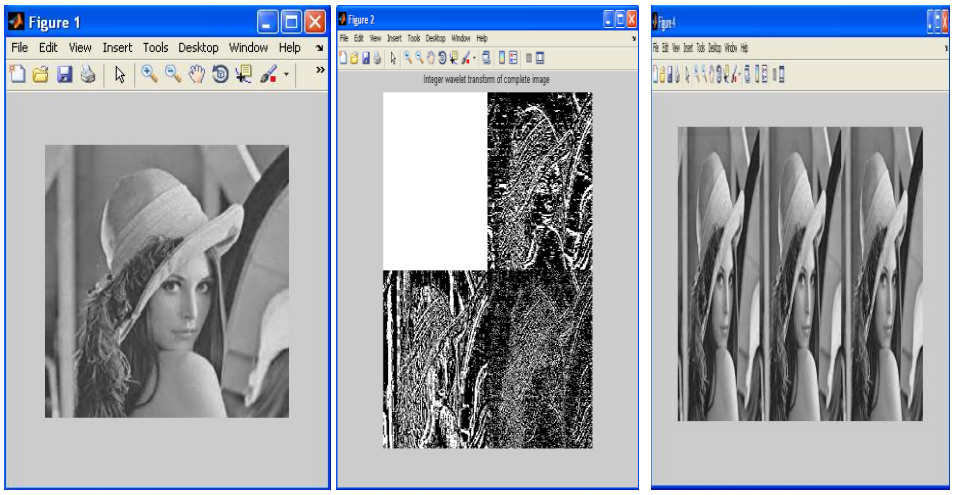


Fig. 6 Processing of Lena image in MATLAB

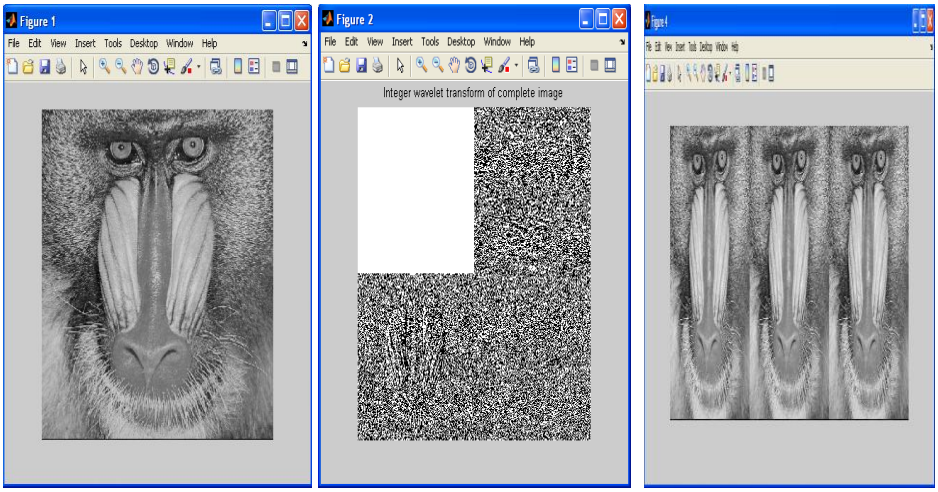


Fig. 7 Processing of Baboon image in MATLAB

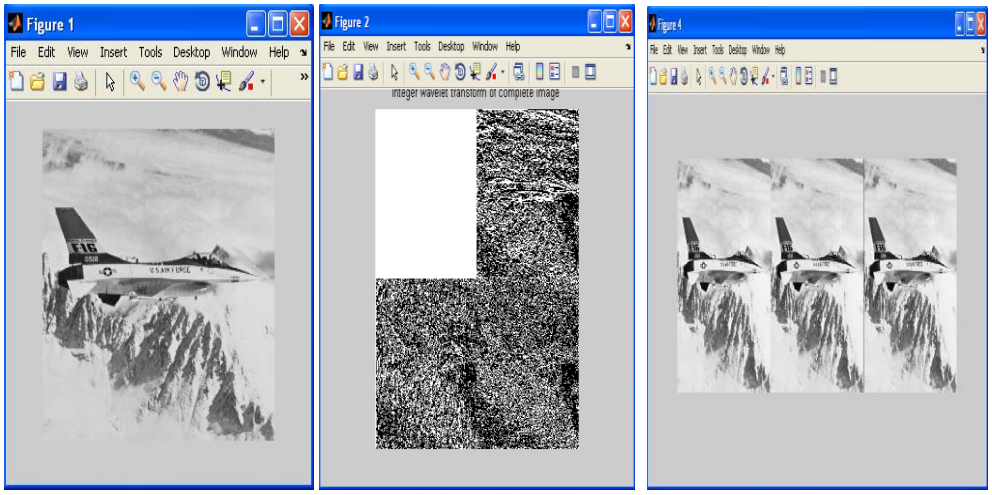


Fig. 8 Processing of Jet image in MATLAB

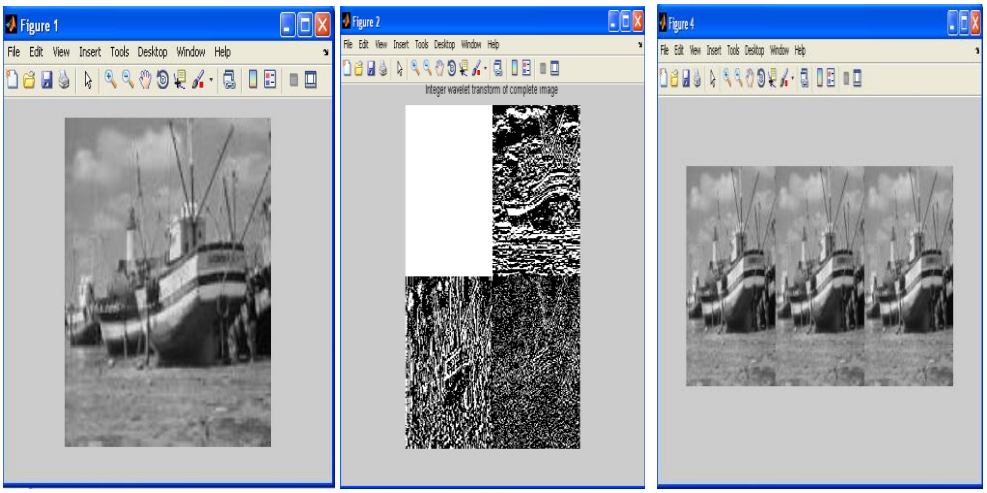


Fig. 9 Processing of Boat image in MATLAB

Table five Comparison of activity capability achieved and therefore the obtained PSNR between our planned technique and strategies in [30, 31, 32 and 33]

Cover Image	Method	Hiding capacity (Bits)	PSNR (DB)
Lena	Proposed	2,13,7696	54.83
	High Capacity [30]	1,048,576	39.94
	Adaptive [31]	986,408	31.8
	HDWT [32]	801,842	33.58
	DWT [33]	573,550	44.90
Baboon	Proposed	2,13,7696	57.83
	High Capacity [30]	1,048,576	40.34
	Adaptive [31]	1,008,593	30.89
	HDWT [32]	883,220	32.69
	DWT [33]	573,392	44.96
Jet	Proposed	2,13,7696	33.51
	High Capacity [30]	1,048,576	45.20
	DWT [33]	573,206	44.76
Boat	Proposed	2,13,7696	54.83
	High Capacity [30]	1,048,576	40.44
	DWT [33]	573,318	44.92

Table five shows the results as compared to previous strategies. We will simply analyze from the table and results that once k up to four, we have a tendency to acquire the upper activity capability and affordable visual quality. So, we have a tendency to take k up to four because the range of bits per pixel.

Conclusions

This work introduced a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding. Genetic algorithm employed to obtain an optimal mapping function to lessen the error difference between the cover and the stego image and use the block mapping method to preserve the local image properties. Also we applied the OPAP to increase the hiding capacity of the algorithm in comparison to other systems. However, the computational complexity of the new algorithm is high. The simulation results showed that capacity and imperceptibility of image had increased simultaneity. Also, we can select the best block size to reduce the computation cost and to increase the PSNR using optimization algorithms such as GA.

The presented work proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines an integer wavelet transform and the optimum pixel adjustment algorithm to maximize the hiding capacity of the system compared to other systems. The proposed system embeds secret information in a random order using a secret key only known to both sender and receiver. It is an adaptive system which embeds different number of bits in each wavelet coefficient according to a hiding capacity function in order to increase the hiding capacity without sacrificing the visual quality of resulting stego image. The proposed system also reduces the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm.

Data hiding using reversible steganography has three primary objectives firstly that steganography should provide the maximum possible payload, and the second, embedded data must be imperceptible to the observer and the original image should be extracted. This steganography method with integer wavelet transform gives high payload (capacity) in the cover image with very little error. This method's performance can be improved by achieving high PSNR and low MSE.

We have introduced a new high capacity Steganography method in wavelet domain. In order to achieve a higher quality of the stego image, we firstly estimate the capacity of each DWT block using the BPCS. The embedding process is then performed over the whole block, rather than in its bit-planes. This approach to the embedding ensures that no noisy bit plane is left unused. Therefore, we achieve a much greater capacity As compared to that offered by previous methods. The proposed approach to the embedding process may also be extended to other transform domains to improve the compromising interrelation between capacity and imperceptibility in image Steganography.

Future work

The PSNR value will be increased by using a different approach with minimum distortion in image quality and methods experimented on audio and video also.

REFERENCES

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

[2] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[3] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[4] Chandramouli, R., Kharerazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[5] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996

[6] Handel, T. & Sandford, M., "Hiding data in the OSI network model", Proceedings of the 1st
International Workshop on Information Hiding, June 1996

[7] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002

[8] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information Hiding – A survey", Proceedings of the IEEE, 87:07, July 1999

[9] C. C. Chang, J. Y. Hsiao, and C. S. Chan, \Finding optimal least significant-bit substitution in image hiding by dynamic programming strategy," Pattern Recognition, vol. 36, no. 7, pp. 1583{1595, 2003.

[10] C. C. Chang and H. W. Tseng, \A steganographic method for digital images using side match," Pattern Recognition Letter, no. 25, pp. 1431{1437, 2004.

[11] L. M. Marevel, C. G. Boncelet, and C. T. Retter, \Spread spectrum image steganography," IEEE Trans. on Image Processing, vol. 8, pp. 1075{1083, Aug. 1999.

[12] C. C. Thien and J. C. Lin, \A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," Pattern Recognition, vol. 36, no. 12, pp. 2875{2881, 2003.

[13] C. K. Chan and L. M. Cheng, Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469{474, Mare. 2004.

[14] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[15] Aretz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001

[16] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998

[17] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April 1998

[18] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security",

Proceedings of the International Conference on Information Technology: Coding and Computing, 2004
[19] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/areticle.pdf
[20] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000
[21] D. C. Lou and J. L. Liu, \Steganographic method for secure communications," Computers and Security, vol. 21, pp. 449{460, Jun. 2002.
[22] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003
[23] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996
[24] C. C. Lin and W. H. Tsai, \Secret image sharing with steganography and authentication," Journal of Systems and Software, vol. 73, pp. 405{414, Nov. 2004.
[25] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998
[26] Marevel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999
[27] Dunbare, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002
[28] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983
[29] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002
[30] Ghasemi E, Shanbehzadeh J, Fassihi N High capacity image steganography using wavelet transform and genetic algorithm. In: Lecture notes in engineering and computer science: proceedings of the international multiconference of engineers and computer scientists 2011, IMECS 2011, Hong Kong, 16–18 March 2011, pp 495–498
[31] C. C. Chang, T. S. Chen, and L. Z. Chung, A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol. 141, pp. 123{138, Mare. 2002.
[32] Lai B, Chang L (2006) Adaptive data hiding for images based on haar discrete wavelet transform. In: Lecture Notes in Computer Science, Springer-verlag Berlin Heidelberg, vol 4319, pp 1085–1093
[33] Chen P, Lin H (2006) A DWT based approach for image steganography. Int J Appl Sci Eng 4(3):275–290