International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 8, October - 2012

Review Of Different Techniques Used In Recent Steganography Researches

Juned Ahmed Mazumder
Research Scholar, Department of Computer Science, Assam University, Silchar

K. Hemachandran
Professor & HOD, Department of Computer Science, Assam University, Silchar

Abstract

As the network technology grows it is necessary to achieve the security of data during communication through the network. In everyday life we use internet for sending our important data through network to the destination but during these communication our important data may accessed by some unauthorized persons so to overcome this problems we can use Steganography for sending our important information. In this paper we have presented a detail look of Steganography and compare Steganography with other security techniques like cryptography and digital watermarking. In this paper we also discussed about different techniques used in recent Steganography researches.

Key-words: Cryptography, Pixel Value Differencing (PVD), Steganography, Steganalysis

1. Introduction

The things that we see may not exactly the same that are! Steganography is the art and science of concealing information to other information. In other words, Steganography is the process of hiding a secret message within a larger one in such a way that no one can know the presence or contents of the hidden message. Steganography will hide the message so there is no knowledge of the existence of the message in the place. Steganography enables us to have a secret communication in modern technology using public channel. The term Steganography is forked from the Greek words "steganos" meaning "cover" and "graphia" meaning "writing" defining it as "covered writing" [1]. In this case any digital media can be used as a carrier for the secret information like text, images, audio or video files. But among those most widely used medium is images because it takes advantage of our limited visual perception of colors and also this field is expected to continually grow as computer graphics power also grows. The following formula provides the description of the steganographic process

Cover_medium + Hidden_data + Stego_key = Stego_medium

In this case the Cover_medium is the file in which we will hide the Hidden_data which may also be encrypted using Stego_key the resultant file is the Stego_medium, the Stego_medium is the same type of file as the Cover_medium that is image, audio or video. Steganalysis on the other hand is an art of identifying the covert communication without disturbing the innocent ones. Its basic requirement is to determine accurately whether a secret message is hidden in the testing medium. Further requirements may include judging the type of the Steganography, estimating the rough length of the message, or even extracting the hidden message[2]. Steganography and steganalysis are in a hide-and-seek game [3]. They try to defeat each other and also develop with each other. Steganalysis does not however consider the successful extraction of the message; this is usually a requirement for cryptanalysis.

2. History

The first recorded uses of steganography can be traced back to 440 BC[4]. The Greek ruler Histaeus employed an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of Steganography. In the same time period, another form of steganography can be traced, in this method the

message was written on a piece of wood after that the wood is covered with wax and then apply a fresh layer of paint. At the receiver end remove the wax from the piece of wood and then reveal the secret information.

The microdots were complete documents, pictures, and plans reduced in size to the size of a period and attached to common paperwork. Null ciphers were also used to pass secret messages. Null ciphers are unencrypted messages with real messages embedded in the current text. Hidden messages were hard to interpret within the innocent messages [4].

Steganography versus Cryptography

Cryptography is also a technique in which we can secure our messages, in Cryptography messages are written in codes. It is the practice and study of techniques for secure communication in the presence of third parties. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography protects information by transforming it into an unreadable format. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. Only those who possess a secret key can decipher (decrypt) the ciphertext into plaintext. On the other hand Steganography hide the existence of secret information so that it cannot be seen by anyone apart from the sender and intended receiver.

There are several ways of classifying cryptographic algorithms [5]. Primarily, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types Cryptography are

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption

Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

3. Steganography versus Watermarking

Information hiding generally relates to both watermarking and Steganography[3]. A watermarking system's primary goal is to achieve a high level of robustness—that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego-medium can destroy it. Speaking of digital image watermarking, we can divide watermarks into two main groups – visible and invisible watermarks.

A visible watermark is a visible semi-transparent text or image overlaid on the original image. It allows the original image to be viewed, but it still provides copyright protection by marking the image as its owner's property. Visible watermarks are more robust against image transformation Thus they are preferable for strong copyright protection of intellectual property that's in digital format. An invisible watermark is an embedded image which cannot be perceived with human's eyes. Only electronic devices (or specialized software) can extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a specialized digital content (text, images or even audio content) to prove its authenticity.

Although the copyright protection is the main field of using digital watermarks, they can also be used for such purposes as advertising (adding company's name and logo as a watermark for promotion rather than for protection) or even adding memo titles to digital photos. It's obvious that only visible watermarks can satisfy these requirements.

4. Classification of Steganography

Image Steganography primarily can be classified into two categories first one is the Image based or spatial domain Steganography and next one is the frequency domain or transform domain Steganography. In spatial domain Steganography we directly deal with the pixel value of the image and insert the secret information into the image by modifying the pixel values of that image. On the other hand in transform domain Steganography before embedding the information into the cover image the image is first transformed into its frequency domain by applying one of the methods suitable for different image formats like First Furrier Transformation, Discreet Cosine Transformation and Wavelet Transformation.

In spatial domain Steganography List Significant Bit (LSB) insertion is the most popular. The basic LSB method has a simple implementation and high capacity [6]. However it has low robustness versus some attacks such as low-pass filtering and compression [7]. Let us consider a simple raster data for 3 pixels (9 bytes) may be re presented as

00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101011

If we want to insert the character A, binary value of which can be represented as 10000001 then it change the 4 bits of the given pixels as shown bellow

00100111 1110100**0** 11001000

0010011**0** 11001000 1110100**0**

1100100**1** 00100111 11101011

In Transform domain Steganography JPEG image Steganography is very popular. In the early stage it was thought that Steganography with JPEG images is not possible since they use lossy compression which results in parts of the image data being altered. But we know that the JPEG compression algorithm is actually divided into lossy and lossless stages. The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain.

5. Different image Steganography methods

From the previous sections we have know about popular Steganography methods like LSB insertion and JPEG Steganography. But we know that for Steganography two parameters are very important first is the security and second is the capacity of embedding information into the cover image. So for achieving more security and capacity we can move towards applying some new techniques into Steganography like genetic algorithm, wavelet transformation etc. In this section we will describe different Image Steganography methods in recent Steganography researches.

A high quality Steganography method with pixel-value differencing and modulus function (2007)

Wang et al.[8], proposed a new image steganographic technique capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye also the new method overcome the problem of falling-off-boundary problem by using pixel-value differencing and the modulus function. First they derive a difference value from two consecutive pixels by utilizing the pixel-value differencing technique (PVD). The hiding capacity of the two consecutive pixels depends on the difference value. This way, the stego-image quality degradation is more imperceptible to the human eye. Second, the remainder of the two consecutive pixels can be computed by using the modulus operation, and then secret data can be embedded into the two pixels by modifying their remainder. In this scheme, there is an optimal approach to alter the remainder so as to greatly reduce the image distortion caused by the hiding of the secret data. The values of the two consecutive pixels are scarcely changed after the embedding of the secret message by the proposed optimal alteration algorithm. Experimental results have also demonstrated that the proposed scheme is secure against the RS detection attack. In the evaluation of experimental result they compare the results of the proposed algorithm with Wu and Tsai's scheme.

Table 1. The results of embedding the same random message by Wu and Tsai's including the proposed methods

Cover Image (512X512)	Wu and Tsai's Method		Proposed Method	
	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)
Lena	51,219	41.1	51,219	44.1
Baboon	57,146	37	57,146	40.3
Peppers	50,907	40.8	50,907	43.3
Jet	51,224	40.6	51,224	43.5
Tank	50,449	42.4	50,449	45.3
Airplane	49,739	42.2	49,739	45.2
Elaine	51,074	41.9	51,074	44.8
Truck	50,065	42.9	50,065	45.6
Couple	51,603	40.2	51,074	44.8
Boat	52,635	38.9	52,635	42.1
Man	52,945	39.1	52,945	42.1
Tiffany	50,920	40.8	50,920	43.9

High-performance JPEG Steganography using complementary embedding strategy (2008)

Liu and Liao [9], proposed a high-performance JPEG steganographic method that adopts the complementary embedding strategy to avoid the detections of several statistical attacks. To show the effectiveness of the proposed method, several statistical attacks are simulated and used to detect the stego-images created by the proposed method. The proposed embedding process is integrated with JPEG encoding process. The raw data of the cover-image is first transformed by DCT. The DCT coefficients are then quantized and rounded to the nearest integers. A stego-key, which provides the major security of the embedding algorithm, is then used to permute the DCT coefficients. The permuted coefficients are then divided into two parts according to a predefined separation ratio

which serves an important parameter to reduce the loss of statistical property of the cover-image resulted from the follow-up secret-bits embedding process. On the other hand, the original message is encrypted to form the secret bits by using a crypto-key. The secret bits are also divided into two parts according to the same separation ratio. Each part of secret bits is embedded in its corresponding part of the permuted non-zero DCT coefficients by using the proposed complementary embedding algorithm. The two parts of the modified coefficients are then combined, de-permutated, and entropy encoded to generate a JPEG stego-image.

The extraction process is also integrated with the JPEG decoding process, and is much simpler than the embedding process. The JPEG stego-image is first entropy decoded to recover the quantized DCT coefficients. The shared stego-key is used to permute these coefficients which are then separated into two parts according to the shared separation ratio. Two parts of secret bits are extracted from their corresponding parts of coefficients respectively, and then combined into a secret-bit sequence. Finally, the shared crypto-key are used to decrypt the secret-bit sequence to recover the original message.

Several experiments have been done to examine the performance of the proposed embedding method. Many standard 512 × 512 gray images with different textural properties were taken as the cover-images. The experimental results are compared with different existing Steganography algorithms as follows

Table 2. Comparison of capacity (in bits) for various embedding algorithms

Test image	Embedding algorithm			
	The proposed	J-Steg	F5	OutGuess
Barb	59 229	45363	45 513	22 699
Boat	50 042	38 374	38 506	19 105
F16	46 079	35 373	35 295	17 721
Goldhill	60 890	45 196	45 505	22 639
Lena	44 131	32 998	33 026	16 375
Mandrill	98 989	75 751	75 837	37 867
Peppers	46 346	34 295	34 074	17 016
Tank	61 220	44 417	44 329	22 195
Tiffany	43 300	31 674	31 516	15 729
Zelda	37 086	27 557	27 630	13 724

High capacity and security Steganography using discrete wavelet transform

Reddy and Raja [10], in this paper High Capacity and Security Steganography using discrete wavelet transform (HCSSD) is proposed. The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. It is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm compared to the existing algorithms. Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter. The result of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients. The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image. In the embedding phase of the method the main idea is wavelet based fusion. It involves merging of the wavelet decomposition of the normalized version of both the cover image and the payload into a single fused result. Normalization is done so that the pixel range of the image lies between 0.0 to 1.0 instead of the integer range (0, 255). Hence we convert the integer range (0, 255) of pixels into floating point values between 0.0 and 1.0. This normalized pixel values is fed as input to the floating point filters which results in reconstruction of the transformed image with better accuracy compared to direct integer values of the pixels as input. Normalization is a process on both the cover image and the payload in order to guarantee pixel values do not exceed their maximum value of one due to modifying

corresponding coefficients of the cover image and payload during fusion. Both cover image and payload is convert into DWT domain. Further, apply DWT on the payload in order to increase the security level. The single fused resultant matrix is obtained, by the addition of wavelet coefficients of the respective sub-bands of the cover image and payload is given by the Equation

$$F(x, y) = \alpha C(x, y) + \beta P(x, y) \quad (1)$$

$$\alpha + \beta = 1 \quad (2)$$

Where F is modified DWT coefficients, C is the original DWT coefficients and P is the approximation band DWT coefficients of the payload. Also alpha and beta are the embedding strength factors. Since alpha and beta are chosen such that the payload is not predominantly seen in the Stego-image obtained in the spatial domain and also for full utilization of the bandwidth of both the Cover Image and the payload. Once fusion is done, apply Inverse Discrete Wavelet Transform (IDWT) followed by renormalization to get the Stego image in the spatial domain.

In extraction phase the Stego-image is normalized, and then DWT is taken. The extraction process involves subtracting the DWT coefficients of the original cover image from the DWT coefficients of the Stego-image. It is then followed by decryption of the subtracted coefficients. Then first step of IDWT on these coefficients is applied followed by second IDWT only with respect to the approximation band of the first IDWT coefficients of the payload. Finally, denormalization is done to get back the payload in spatial domain. For performance analysis authors considered the Cover Images (CI) such as Lady, Aero plane, Players, Cow boys and Flower. Payload images (PL) are Flower, Bank text, Astronauts, Dog and Elephant. The payload is embedded into the cover image to derive the Stego image at the sending end. The payload is recovered from the Stego image at the destination with minimum distortion. The following table gives the details of the experimental results.

Table 3. Experimental Results of the given method

Images	Type	Size	MSE	PSNR	Entropy
Lady Flower	JPEG JPEG	346×396 240×240	0.17	55.6	0.00019
Aero plane Bank Text	TIFF PNG	400×300 810×400	2.76	43.7	0.0000
Player Astronauts	JPEG PNG	400×300 200×200	0.9	48.1	0.0004
Cow Boys Dog	JPEG TIFF	186×100 436×600	0.17	55.58	0.0000
Flower	JPEG	200×150	0.98	48.20	0.0000

A Secure Steganography Method based on Genetic Algorithm (2010)

Wang et al.[11], in this paper a novel Steganography algorithm was proposed. The genetic algorithm is used to estimate the best adjusting mode. By the adjustment, the artifacts caused by the Steganography can be eliminated and the image quality will not be degraded. Genetic algorithm is used to search for a best adjustment matrix. Genetic algorithm is a general optimization algorithm. It transforms an optimization or search problem as the process of chromosome evolution. When the best individual is selected after several generations, the optimum or sub-optimum solution is found. The three most important operations of genetic algorithm are reproduction, crossover and mutation. The adaptive values affect the copy operation. In general, the individuals with larger fitness values have higher possibilities to be selected to breed the next generation. After embedding the secret message in Cover image by LSB. The adjustment is proceeded as follows: Firstly, the stego-image is divided into 8X8 blocks. Secondly, the blocks are classified and labeled as follows

1. For a block B, apply the non-positive flipping F- and the non-negative flipping F+ on the block. The flipping mask M+ and M- are generated randomly. The result is B+ and B-
2. calculate f(B+), f(B-) and f(B).
3. do step 1 and 2 5000 times. Define four variables to categorize the blocks by comparison of f(B+), f(B-) and f(B).
   - P_{+R}, the count of the occurrence when the block is regular under the non-negative flipping.
   - P_{+S}, the count of the occurrence when the block is singular under the non-Negative flipping.
   - P_{-R}, the count of the occurrence when the block is regular under the non-positive flipping
   - P-S, the count of the occurrence when the block is singular under the non-positive flipping.
4. Compare P+R to P+S and P-R to P-S, and the labels of the block are determined:
   - R+, if P+R=P+S > 1:8.
   - S+, if P+S=P+R > 1:8.
   - R-, if P-R=P□S > 1:8.
   - S-, if P-S=P□R > 1:8.
5. At last, the blocks are categorized into 4 groups R_+R_-, R_+S_-, S_+R_-, S_+S_-.

A Data Embedding Technique for Gray scale Image Using Genetic Algorithm (DEGGA) (2011)

Mandal and Khamrui[12], proposed an authentication/data hiding technique through steganographic approach termed as DEGGA using Genetic Algorithm. In DEGGA insertion is made by choosing image mask in row major order. The dimension of the authenticating image is extracted first. A 3x3 mask is chosen from the host image. The dimension of the authenticating image along with the authenticating image is embedded into the host image. Genetic Algorithm is applied onto the embedded image to enhance a layer of security. Mutation procedure is applied on the embedded image onto the rightmost k bits by consecutive bitwise XOR operation on k steps and taking the MSB of the intermediate stream generated in each step. A method of bit handling is applied to keep the fidelity high. In the process of embedding dimension of the authenticating image followed by the content of the message/authenticating image. This scheme use gray scale image for secure message transmission. An authenticating image of size m x n is chosen. The size of the host image is pxq.

Input: Host image of size pxq, authenticating image of size pxq.

Output : Embedded image of size pxq.

Method: Insertion of authenticating image bitwise into the source image.

Algorithm:

Step1: Obtain the size of the authenticating image m x n.

Step2: For each authenticating message/image, Read source image block of size 3x3 in row major order. Extract authenticating message/image bit one by one. Replace the authenticating message/image bit in the rightmost 4 bits within the block, four bits in each byte.

Step3: Read one character/ pixel of the authenticating message/ image at a time.

Step4: Repeat step 2 and 3 for the whole authenticating message/ image size, content.

Step 5: Perform mutation operation for the whole embedded image. For mutation rightmost 3 bits from each bytes is taken. A consecutive bitwise XOR is performed on it for the 3 steps. It will form a triangular form and first bit from each step is taken.

Step 6: A bit handling method is performed on the embedded image. If the difference between the host and embedded image is +/-16 then 16 will be added to the embedded image to keep intact the visibility of the embedded image.

Step 7: Stop

Reverse process is followed during decoding. Genetic algorithm is used to enhance a security level. Various statistical parameters computed are compared with the existing genetic algorithm based Steganography algorithm.

Table 4. Experimental results of the algorithm is as follows

Host Image	Embedding Image	PSNR	MSE
Baboon	Jet	34.826	21.40
Baboon	Scene	34.804	21.511
Baboon	Tiff	34.830	21.38
Lena	Jet	34.826	21.399
Lena	Scene	34.803	21.513
Lena	Tiff	34.821	21.425

Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation (2011)

Mohamed et al.[13], in this paper a hybridization technique was proposed for Steganography by incorporates LSB technique with a key-permutation method. The paper also proposed an optimal key permutation method using genetic algorithms for best key selection. Both normal and optimized methods are tested with standard images, varying both data size as well as key space.

To prevent illicit access of the data and obtain better embedding results, a key-permutation method with an optimal LSB substitution method is presented. A random key is generated and then distributed to the communication parties. Before embedding the data into the LSB of the cover image, it is represented with the help of the key (encrypted) at the sending end; an opposite operation is then performed at the receiving end to reveal the secret data. Optimization of the key is another phase of the proposed model. It is achieved by selecting best embedding results for a set of all possible keys using genetic algorithms. To obtain the optimal embedding result, the simplest method is to calculate the PSNR for each substitution, and select the one having the maximum PSNR as the optimal result. Hence, it is very impractical and time Consuming for us to compute the PSNR for each permutation. A genetic algorithm is thus developed to solve this problem, where GA is a randomized search procedure that is commonly used to solve the optimization problems. A solution in the problem domain corresponds to an individual in a GA, which is represented by a chromosome containing many genes. An objective function called the fitness function is used

to evaluate the quality of each chromosome. In general, GA is mainly comprised of the following three operators, namely, (1) reproduction, (2) crossover, and (3) mutation. Reproduction retains the current chromosome's genes, crossover assembles existing genes into new combinations, and mutation produces new genes. The procedure of GA is started by specifying an initial population in the first generation, and during each next generation, the individuals in the population undergo the activities of reproduction, Crossover and mutation, to produce their offspring. Then a fitness function is applied to each offspring to determine its quality. The individuals with high quality will survive and form the population of the next generation. The process will repeat for many times until a predefined requirement is satisfied, or a constant number of iterations are exceeded. Final experimental results show decrement in computation time when increasing number of keys, at the same time system security improves.

High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm (2011)

Ghasemi et al.[14], proposed a method by the application of Wavelet Transform and Genetic Algorithm in a novel Steganography scheme. They employ a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message. Here frequency domain used to improve the robustness of Steganography and implement Genetic Algorithm and Optimal Pixel Adjustment Process to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions. In this proposed algorithm Haar wavelet transform is used which has the capability to offer some information on frequency-time domain simultaneously. In this transform, time domain is passed through low-pass and high-pass filters to extract low and high frequencies respectively. This process is repeated for several times and each time a section of the signal is drawn out. DWT analysis divides signal into two by signal decomposition for various frequency bands and scales. DWT utilizes two function sets: scaling and wavelet which associate with low and high pass filters orderly. Such a decomposition manner bisects time separability. In other words, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability.

The following steps explain the embedding process of the proposed algorithm

Step1. Divide the cover image into 4x4 blocks.
Step2. Find the frequency domain representation of blocks by 2D Haar Discrete Wavelet Transform and get four subbands LL1, HL1, LH1, and HH1.
Step3. Generate 16 genes containing the pixels numbers of each 4x4 blocks as the mapping function.
Step4. Embed the message bits in k-LSBs DWT coefficients each pixel according to mapping function. For selecting value of k, images are evaluated from k=3 to 6. K equal to 1 or 2, provide low hiding capacity with high visual quality of the stego-image and k equal to 7 or 8, provide low
visual quality versus high hiding capacity.
Step5. Fitness evaluation is performed to select the best mapping function.
Step6. Apply Optimal Pixel Adjustment Process on the image.
Step7. Calculate inverse 2D-HDWT on each 4x4 block.

The extraction algorithm consists of four steps as follows:

Step1. Divide the cover image into 4x4 blocks.
Step2. Extract the transform domain coefficient by 2D HDWT of each 4x4 block.
Step3. Employ the obtained function in the embedding phase and find the pixel sequences for extracting.
Step4. Extract k-LSBs in each pixel.

The proposed method is applied on 512x512 8-bit grayscale images "Jet", "Boat", "Baboon" and "Lena". The messages are generated randomly with the same length as the maximum hiding capacity. The following table shows the stego-image quality by PSNR.

Table 5. Experimental Results

Cover image	PSNR			
	K=3	K=4	K=5	K=6
Lina	46.83	39.94	32.04	24.69
Jet	51.88	45.20	37.45	29.31
Boat	48.41	40.44	31.17	23.60
Baboon	47.32	40.34	32.79	24.80

Combining jpeg Steganography and Substitution encryption for secure data Communication (2012)

Lasker and Hemachandran[15], proposed a method for hiding large volumes of data in digital images by combining cryptography and steganography while incurring minimal perceptual degradation in terms of human visual interpretation and to solve the problem of unauthorized data access. In this method first encrypt a message using substitution cipher method and then embed the encrypted message inside a JPEG image using DCT in frequency domain. A substitution cipher is one in which each character in the plaintext is substituted for another character in the

ciphertext. Thus the original message that is represented in such a form that is not meaningful to the third party. JPEG compression is based on the discrete cosine transform (DCT) and reduces the visual redundancy to achieve good compression performance. Thus it is very difficult to detect hidden message in frequency domain and for this reason transformation like DCT was used in the proposed algorithm. Therefore, the embedding capacity provided by JPEG steganography is less prone to detection. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, it would still require the cryptographic decoding method to decipher the encrypted message. The intended receiver should be able to recover the embedded data successfully, without any errors. The proposed methods can be employed for applications that require high-volume embedding with robustness against attacks. For evaluating result with the proposed algorithm authors used four images which are "tulips", "winter" and "sunset" , the following table shows the MSE and PSNR values for original and stego images.

Table 6. Experimental Result shows MSE and PSNR of original and stego-image

Cover Image	Stego Image	No. of bytes embedded	MSE %	PSNR (dB)	No. of bytes extracted
Tulips	Stego_tulips	2213 bytes	6.22	40.19	2213 bytes
Winter	Stego_winter	1628 bytes	3.54	42.63	1628 bytes
Sunset	Stego_sunset	1323 bytes	1.71	45.79	1323 bytes

Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images through Exclusion of Overflow/Underflow (2012)

Mandal and Das[16], proposed an adaptive steganography based on modified pixel-value differencing through management of pixel values within the range of gray scale PVD method is used and check whether the pixel value exceeds the range on embedding. Positions where the pixel exceeds boundary has been marked and a delicate handle is used to keep the value within the range. In PVD method pixel values in the stego image may exceed the gray scale range which is not desirable as it may leads to improper visualization of the stego image. In this paper they introduced a method to overcome this problem. In the proposed method they have used the original PVD method to embed secret data. If any pixel value exceeds the range (0 to 255), then check the bit stream 't' to be hidden. If MSB(most significant bit) of the selected bit stream 't' is 1 then embed one less number of bits, where MSB position is discarded from t; otherwise the bit number of hidden data depends on w_i . For instance, if pixel value exceeds the range and selected bit stream t=101, then set t=01 and embed it. If it is seen that the pixel value again exceeding range, then embed the value at one pixel, rather than both pixels(of the pixel block), which will not exceed the range after embedding; where the other pixel is kept unchanged. It will keep the pixel values within the range because both pixels of a block cannot exceed at the same time as per the PVD method by Wu and Tsai. Keep the information within each block, whether one less bit is embedded or not, as overhead. The problem of overshooting gray-level range in PVD has been removed which results no effect on hiding capacity. C programming language is used to implement the proposed algorithm. The range table width used here are w_i ={ 8, 8, 16, 32, 64, 128 }. Here cover images of size 512*512 and hide a digital image as the secret information have used and also used the Peak-Signal-to-Noise ratio (PSNR) to evaluate the quality of stego-image. In the experimental results PSNR values are changing between -0.62 to +0.32 dB and capacity remains same compared to original PVD method. According to the proposed method, if pixel value exceeds gray scale range, one bit is discarded from the selected bit-stream to be hidden. So, decimal value of the reduced bits will be half or less than half. As a result the distortion of the pixel value in the stego-image will be less. On the other hand, for keeping the overhead information adding or subtracting of some values with the pixel values takes place. This can increase the distortion of the image.

6. Conclusion

More over there are various methods of Steganography, in this paper only the recent techniques of image Steganography were discussed. Each method of Steganography have some advantages and disadvantages according to the image file formats used so depending on the file formats like JPEG, BMP, GIF, JPEG2000, PNG etc we can use different kind of Steganography methods to different file formats. Security and capacity are considered to be the two main factors for Steganography methods and from the above discussion we can say that techniques like

Genetic Algorithm, Wavelet transformation and Pixel Value Difference (PVD) can provide better security and Capacity for image Steganography.

8. References

[1] S. Katzenbeisser, F.A.P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking" Artech House, Norwood, MA, 2000

[2] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing ©2011 ISSN 2073-4212, Volume 2, Number 2, April 2011

[3] Niels Provos and Peter Honeyman, "Hide and seek: An introduction to Steganography" IEEE Security and Privacy, vol. 1, no.3, pp. 32-44, 2003.

[4] A.Joseph Raphael,Dr.V Sundaram, "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[5] Gary C. Kessler, "An Overview of Cryptography", Handbook on Local Area Networks, published by Auerbach in September 1998.

[6] Frank Y. Shih, Yi-Ta Wu. "Digital Steganography Based on Genetic Algorithm. Handbook of Research on Secure Multimedia Distribution," DOI: 10.4018/978-1-60566-262-6.ch023. 2011

[7] R. J. Anderson and Fabien A. P. Petitcolas, "On the limits of steganography", IEEE Journal on Selected Areas in Communications", vol. 16, no. 4, pp. 474-481, 1998

[8] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function", The Journal of System and Software. 2007

[9] Chiang-Lung Liu, Shiang-Rong Liao, "High-performance JPEG steganography using complementary embedding Strategy", Pattern Recognition 41 (2008) 2945 – 2955, 2008

[10] H S Manjunatha Reddy, K B Raja, "HIGH CAPACITY AND SECURITY STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6)

[11] Shen Wang, Bian Yang and Xiamu Niu, "A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing c 2010 ISSN 2073-4212 Volume 1, Number 1, January 2010

[12] J. K. Mandal, A. Khamrui, "A Data Embedding Technique for Gray scale Image Using Genetic Algorithm (*DEGGA*)", International Conference on Electronic Systems (ICES-2011)

[13] Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf, "Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation", International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011

[14] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", International Multi conference of Engineers and Computer Scientists 2011 vol I, ISBN-978-988-18210-3-4,2

[15] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "COMBINING JPEG STEGANOGRAPHY AND SUBSTITUTION ENCRYPTION FOR SECURE DATA COMMUNICATION", David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 149–160, 2012.© CS & IT-CSCP 2012

[16] J. K. Mandal and Debashis Das, "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow", David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 93–102, 2012. © CS & IT-CSCP 2012

[17] Shanthini, B. and S. Swamynathan, "Multimodal Biometric-based Secured Authentication System using Steganography", Journal of Computer Science 8 (7): 1012-1021, 2012

[18] Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal, "A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method(WMM)", International Journal of Computer and Information Engineering 4:2 2010

Authors

Juned Ahmed Mazumder received his M.Sc. (Computer Science, 5 years integrated course) degree with first class in 2011 from Assam University, Silchar, where he is currently doing his Ph.D. His research interest includes Image Processing, Steganography, Neural Network and Data Security.

Prof. K. Hemachandran is associated with the Department of Computer Science, Assam University, Silchar, since 1998. Currently he is serving as the Head of the Department in the Department of Computer Science, Assam University, Silchar. He obtained his M.Sc. Degree from Sri Venkateswara University, Tirupati and M.Tech and Ph.D Degrees from Indian School of Mines, Dhanbad. His areas of research interest are Image Processing, Software Engineering and Distributed Computing.