International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:8, 2010

A Data Hiding Model with High Security Features Combining Finite State Machines and PMM method

Souvik Bhattacharyya and Gautam Sanyal

Abstract—Recent years have witnessed the rapid development of the Internet and telecommunication techniques. Information security is becoming more and more important. Applications such as covert communication, copyright protection, etc, stimulate the research of information hiding techniques. Traditionally, encryption is used to realize the communication security. However, important information is not protected once decoded. Steganography is the art and science of communicating in a way which hides the existence of the communication. Important information is firstly hidden in a host data, such as digital image, video or audio, etc, and then transmitted secretly to the receiver.In this paper a data hiding model with high security features combining both cryptography using finite state sequential machine and image based steganography technique for communicating information more securely between two locations is proposed. The authors incorporated the idea of secret key for authentication at both ends in order to achieve high level of security. Before the embedding operation the secret information has been encrypted with the help of finite-state sequential machine and segmented in different parts. The cover image is also segmented in different objects through normalized cut.Each part of the encoded secret information has been embedded with the help of a novel image steganographic method (PMM) on different cuts of the cover image to form different stego objects. Finally stego image is formed by combining different stego objects and transmit to the receiver side. At the receiving end different opposite processes should run to get the back the original secret message.

Keywords—Cover Image, Finite state sequential machine,Melay machine,Pixel Mapping Method (PMM), Stego Image,NCUT.

I. Introduction

STEGANOGRAPHY is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography means "covered writing" in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only. A famous illustration of steganography is **Simmons' Prisoners' Problem** [20].An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as then the secret key steganography where as pure steganography means that there is none prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [2], [3] and [10].For a more thorough knowledge of steganography methodology the reader may see [16], [21].Some Steganographic model with high security features has been presented in [4], [5] and [6].Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [21]. Fig. 1 below shows the different categories of steganography techniques.

S. Bhattacharyya is with the Department of Computer Science and Engineering, University Institute of Technology, The University of Burdwan, West Bengal, India e-mail: (souvik.bha@gmail.com).

G. Sanyal is with with the Department of Computer Science and Engineering, National Institute of Technology West Bengal, India e-mail: (gautam.sanyal@cse.nitdgp.ac.in).

Fig. 1. Types of Steganography

A block diagram of a generic image steganographic system is given in Fig. 2.

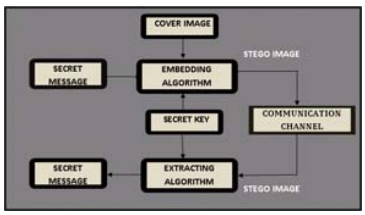

Fig. 2. Generic form of Image Steganography

A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message.

In this paper a specific secret-key image based data hiding model has been proposed which uses an image as the cover data and the secret information is embedded in the cover to form the stego image. Before embedding the secret information has been encoded with the help of finite state sequential machine.The cover image has been divided into several segments using normalized cut.Each segment of the encoded message has been embedded at each segments of the

cover image through PMM method to form the stego objects. Stego image will be formed combining the stego objects. This work proposes a novel algorithm with higher security features so that the embedded message can not be hacked by unauthorized user. This paper has been organized as following sections: Section II describes the proposed cryptography technique using Sequential Machine.Section III describes the normalized cut technique.Section IV deals with some related works, Section V deals with proposed method. Experimental results are shown in Section VI. Section VII contains the analysis of the results and Section VIII draws the conclusion.

II. Cryptography Using Sequential Machine

For a finite-state sequential machine, the output depends not only on the input as well as the previous state of the machine. Thus a finite-state sequential machine can be used in cryptography where the input data stream is the input to the sequential machine and the state determines the output input relationship along with the next state. Here the authors use the input state of the sequential machine as the input sequence and then use the data as an input to the sequential machine. The next transition state can be used as the encrypted data and the output can be used as the key.Melay machine has been used here for producing the encrypted form of the input signal.

A. Finite-state machine (FSM)

A finite-state machine (FSM) or finite-state automaton (plural: automata), or simply a state machine, is a mathematical abstraction sometimes used to design digital logic or computer programs. It is a behavior model composed of a finite number of states, transitions between those states, and actions, similarly to a flow graph in which one can inspect the way logic runs when certain conditions are met. It has finite internal memory, an input feature that reads symbols in a sequence, one at a time without going backward; and an output feature, which may be in the form of a user interface, once the model is implemented. The operation of an FSM begins from one of the states (called a start state), goes through transitions depending on input to different states and can end in any of those available, however only a certain set of states mark a successful flow of operation (called accept states).

B. Mathematical model of FSM

In accordance to the general classification, the following formal definitions are found: A deterministic finite state machine or acceptor deterministic finite state machine is a quintuple $(\sum, S, s0, \delta, F)$, where:

- $\sum$ is the input alphabet (a finite, non-empty set of symbols).
- S is a finite, non-empty set of states.
- s0 is an initial state, an element of S.
- δ is the state-transition function: $\delta : S \times \Sigma \rightarrow S$(in a nondeterministic finite state machine it would be $\delta : S \times \Sigma \rightarrow \mathcal{P}(S)$, i.e., δ would return a set of states).
- F is the set of final states, a (possibly empty) subset of S.

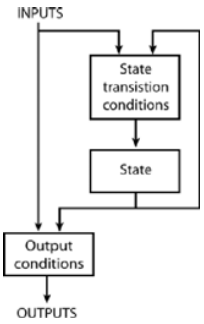

Fig. 3. Finite State Machine

C. Mealy machine

In the theory of computation, a Mealy machine is a finite state transducer that generates an output based on its current state and input. This means that the state diagram will include both an input and output signal for each transition edge. In contrast, the output of a Moore finite state machine depends only on the machine's current state; transitions are not directly dependent upon input. Mealy machines provide a rudimentary mathematical model for cipher machines. Considering the input and output alphabet the Latin alphabet, for example, then a Mealy machine can be designed that given a string of letters (a sequence of inputs) can process it into a ciphered string (a sequence of outputs). A Mealy machine is a 6-tuple, $(S, S0, \sum, \Lambda, T, G)$, consisting of the following:

- a finite set of states (S).
- a start state (also called initial state) S0 which is an element of (S).
- a finite set called the input alphabet $(\sum)$.
- a finite set called the output alphabet (Λ).
- a transition function $(T : S \times \sum \rightarrow S)$ mapping pairs of a state and an input symbol to the corresponding next state.
- an output function $(G : S \times \sum \rightarrow \Lambda)$ mapping pairs of a state and an input symbol to the corresponding output symbol.

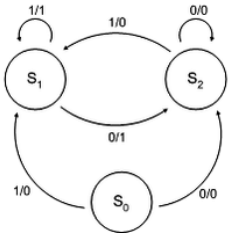

Fig. 4. Melay Machine

III. Extraction of cuts through Normalized Cut

Shi and Malik [18], [19] proposed the Normalized Cuts algorithm for solving image segmentation problem, which is treated as a graph partitioning problem. The normalized cut criterion measures both the total dissimilarity between the different groups as well as the total similarity within

the groups. An efficient computational technique based on a generalized eigen value problem can be used to optimize this criterion. Algorithm of Normalized Cut: A Graph G = (V, E) can be partitioned into two disjoint sets, A and B.

Fig. 5. Cuts in a GRAPH

The degree of dissimilarity between these two pieces can be computed as: $cut(A, B) = \sum_{u \epsilon A, v \epsilon B} w(u, v)$.

The normalized cut (NCUT) is defined as: $N_{cut}(A, B) = \frac{cut(A,B)}{asso(A,V)} + \frac{cut(A,B)}{asso(B,V)}$ where $asso(A, V) = \sum_{u \epsilon A, t \epsilon V} w(u, t)$.

IV. Related Works

A. Some Data Hiding Method using Steganography

1) Data Hiding by LSB : Various techniques about data hiding have been proposed in literatures. One of the common techniques is based on manipulating the least-significant-bit (LSB) [8], [9] and [15], [17]planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression.

2) Data Hiding by PVD : The pixel-value differencing (PVD) method proposed by Wu and Tsai [22] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification. In the extraction phase, the original range table is necessary. It is used to partition the stego-image by the same method as used to the cover image. Based on PVD method, various approaches have also been proposed. Among them Chang et al. [14]proposes a new method using tri-way pixel-value differencing which is better than original PVD method with respect to the embedding capacity and PSNR.

3) Data Hiding by GLM : In 2004, Potdar et al.[11] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

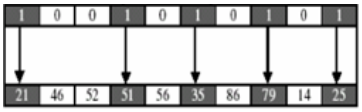

Fig. 6. Data Embedding Process in GLM

Fig. 7. Data Extraction Process in GLM

4) Data Hiding by the method proposed by Ahmad T et al.: In this work [1] a novel Steganographic method for hiding information within the spatial domain of the grayscale image has been proposed. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel.

B. Some Data Hiding Model

1) High capacity image steganographic model: An image steganographic model [23] is proposed here that is based on variable-size LSB insertion to maximize the embedding capacity while maintaining image fidelity. For each pixel of a gray-scale image, at least four bits can be used for message embedding. Three components arc provided to achieve the goal. First, according to contrast and luminance characteristics, the capacity evaluation is provided to estimate the maximum embedding capacity of each pixel. Then the minimum-error replacement method is adapted to find a gray scale as close to the original one as possible. Finally, the improved gray scale compensation, which takes advantage of the peculiarities of human visual system, is used to eliminate the false contouring effect. Two methods, pixel wise and bit wise, are provided to deal with the security issue when using the proposed model.

2) A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images: In this paper [13] an image based steganography model has been presented that that combines Least Significant Bit(LSB), Discrete Cosine Transform(DCT), and compression techniques on raw images to enhance the security of the payload. Initially, the LSB algorithm is used to embed the payload bits into the cover image to derive the stego-image. The stego-image is transformed from spatial domain to the frequency domain using DCT. Finally quantization and run length coding algorithms are used for compressing the stego-image to enhance its security. It is observed that secure images with low MSE and BER are transferred without using any password, in comparison with earlier works.

3) Hiding a Large Amount of Data with High Security Using Steganography Algorithm: This study [12] deals with constructing and implementing new algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image. Author has used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather

than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. This concept based on both visual and statistical. High security layers have been proposed here through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. Here the results against statistical and visual attacks are discussed and make comparison with the previous Steganography algorithms like S-Tools. Here authors have shown that the proposed algorithm can embed efficiently a large amount of data that has been reached to 75 percent of the image size with high quality of the output.

V. Proposed Method

This section is divided into three subsections namely Data Encryption through Melay machine,Data Hiding using PMM and Proposed model of data hiding using the above two.

A. Proposed Method for Encryption

Consider the following state transition table of the proposed sequential machine.Here the states are S=(Q_0, Q_1, Q_2, Q_3),Input alphabet $\sum$=(0,1),Output alphabet (Λ)=(0,1).Fig 8 and 9 respectively shows the state transition table and state transition diagram of the proposed sequential machine.

Current State	Next State			
	Input 0		Input 1	
	STATE	OUTPUT	STATE	OUTPUT
Q_0 (00)	Q_0	0	Q_1	0
Q_1(01)	Q_3	1	Q_2	1
Q_2(10)	Q_2	1	Q_3	1
Q_3(11)	Q_1	0	Q_0	0

Fig. 8. State Transition Table for the Sequential Machine

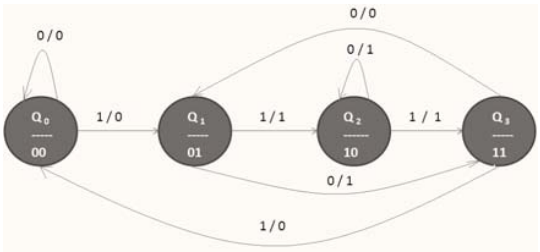

Fig. 9. State transition diagram for the Sequential Machine

B. Proposed Method for Data Hiding (PMM)

In this section the authors propose a new method for information hiding within the spatial domain of any gray scale image.This method can be considered as the improved version of [7].The input messages can be in any digital form, and are often treated as a bit stream. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbors lies at the boundary of the image or not. Data embedding are done by mapping each four bits of the secret message in each of the neighbor pixel based on some features of that pixel. Fig.10 shows the mapping information for embedding four bits per pixel.

MSG BIT SEQ	2nd SET - RESET BIT	3rd SET - RESET BIT	PIXEL INTENSITY VALUE	NO OF ONES(BIN)
0000	EVEN	EVEN	EVEN	EVEN
0001	EVEN	EVEN	EVEN	ODD
0010	EVEN	EVEN	ODD	EVEN
0011	EVEN	EVEN	ODD	ODD
0100	EVEN	ODD	EVEN	EVEN
0101	EVEN	ODD	EVEN	ODD
0110	EVEN	ODD	ODD	EVEN
0111	EVEN	ODD	ODD	ODD
1000	ODD	EVEN	EVEN	EVEN
1001	ODD	EVEN	EVEN	ODD
1010	ODD	EVEN	ODD	EVEN
1011	ODD	EVEN	ODD	ODD
1100	ODD	ODD	EVEN	EVEN
1101	ODD	ODD	EVEN	ODD
1110	ODD	ODD	ODD	EVEN
1111	ODD	ODD	ODD	ODD

Fig. 10. Mapping Technique for data embedding

Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operations has been carried out to get back the original information.

Algorithms for Embedding and Extraction: Let C be the original 8 bit gray scale image of size N x N i.e. C = $(P_{ij} \mid 0 \leq i < N, 0 \leq j < N, P_{ij} \in 0, 1, \ldots, 255)$. Let MSG be the n bit secret message represented as MSG =$(m_k \mid 0 \leq k < n, m_k \in 0, 1)$.A seed pixel P_{rc} can be selected with row (r) and column (c). Next step is to find the 8 neighbors $P_{r'c'}$ of the pixel P_{rc} such that $r' = r + l$, $c' = c + l$,$-1 \leq l \leq 1$. The embedding process will be finished when all the bits of every bytes of secret message are mapped or embedded.

Algorithm of the Data Embedding method are described as :

- Input : Cover Image(C), Message (MSG).
- Find the first seed pixel P_{rc}.
- $count = 1$.
- while ($count \leq n$)
- begin (for embedding message in message surrounding a seed pixel).
- m_k=Get next msg bit.
- $count = count + 1$.
- Mask the 5TH bit from left with the m_k in 'Bincvr'
- m_{k+1}=Get next msg bit.
- $count = count + 1$.
- Mask the 6TH bit from left with the m_{k+1} in 'Bincvr'
- cnt=Count number of ones of one of the $P_{r'c'}$ of intensity (V).
- m_{k+2}=Get next msg bit.
- $count = count + 1$.
- m_{k+3}=Get next msg bit.
- $count = count + 1$.
- Bincvr= Binary of V.
- If($m_{k+2} = 0$ & $m_{k+3} = 1$)
- $Bincvr(zerothbit) = 0$

- If($cnt \bmod 2 = 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- If($m_{k+2} = 0$ & $m_{k+3} = 0$)
- $Bincvr(zerothbit) = 1$
- If($cnt \div 2 \neq 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- If($m_{k+2} = 0$ & $m_{k+3} = 0$)
- $Bincvr(zerothbit) = 0$
- If($cnt \bmod 2 \neq 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- If($m_{k+2} = 0$ & $m_{k+3} = 1$)
- $Bincvr(zerothbit) = 1$
- If($cnt \bmod 2 = 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- End
- Get the next neighbor pixel $P_{r'c'}$ for embedding based on previous $P_{r'c'}$ and repeat.
- End
- Return the stego image (S).

Algorithm of the Data Extraction Method : The process of extraction proceeds by selecting those same pixel with their neighbors. The extracting process will be finished when all the bits of every bytes of secret message are extracted. Algorithm of the extraction method are described as :

- Input : Stego image (S) , count.
- $count = count \div 2$.
- BinMsg= " ".
- Find the first seed pixel P_{rc}.
- I=0.
- While ($count \leq N$)
- begin (for extract message in message around a seed pixel).
- Get the (First/Next) neighbor pixel $P_{r'c'}$.
- cnt=Count number of ones of one of the $P_{r'c'}$ of intensity (V).
- Bincvr= Binary of V.
- Binmsg(i)=3rd Bit of Bincvr from Right.
- $i = i + 1$.
- Binmsg(i)=2nd Bit of Bincvr from Right.
- $i = i + 1$.
- Binmsg(i)=ZerothBit of Bincvr.
- $i = i + 1$.
- If (cnt mod 2 = 0) (i.e. it is even) Binmsg(i)=0 Else Binmsg(i)=1
- Binmsg(i)=Enters according to One of ones in the intensity(1 for odd :0 for even).
- $i = i + 1$.
- $count = count + 1$.
- End.
- Get the next neighbor pixel $P_{r'c'}$ for embedding based on previous $P_{r'c'}$ and repeat.
- End loop.
- Binmsg is converted back to Original message.
- Return Original Message.
- End.

One important point needs to be kept in mind that a specific order for selecting the neighbor pixels has to be maintained for embedding / mapping process and also for the process of extraction other wise it would not be possible for retrieve the data in proper sequence. This sequence has been shown in figure 11

.

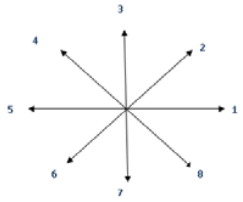

Fig. 11. Sequence of data embedding

Algorithm for Pixel Selection Method : Random Pixel Generation for embedding message bits is dependent on the intensity value of the previous pixel selected.It includes a decision factor (dp) which is dependent on intensity with a fixed way of calculating the next pixel.The algorithm for selection of pixel for embedding is described below:

- Input: C , previous pixel position (x,y),pixel intensity value (v).
- Consider dp (Decision Factor)=1 if ($intensity \leq 80$),dp=2 if ($intensity \geq 80$ & ≤ 160) ,dp=3 if ($intensity > 160$ & ≤ 255).
- $t = x + 2 + dp$
- if $(t \geq N) m = 2, n = y + 2 + dp$
- else $m = x + 2 + dp, n = y$
- Return m and n.
- End

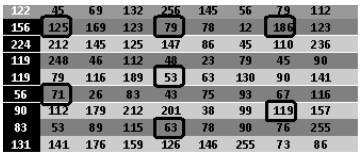

Fig. 12. Snapshot of Selected Pixel for embedding.

C. Proposed Data Hiding Model

Fig. 13 shows the block diagram of the proposed secret-key image steganographic model. The input messages can be in any digital form, and are often treated as a bit stream. The input message is first converted into encrypted form through proposed encryption method. This encrypted message generates the secret key which may be used as a password before starting of the embedding or extracting operation for increasing another level of security.Embedding in the cuts of the cover image is done through proposed PMM method.

VI. Experimental Results

This section presents the obtained results via different processes mentioned in the proposed model.Results of the proposed data hiding method has been shown based on two

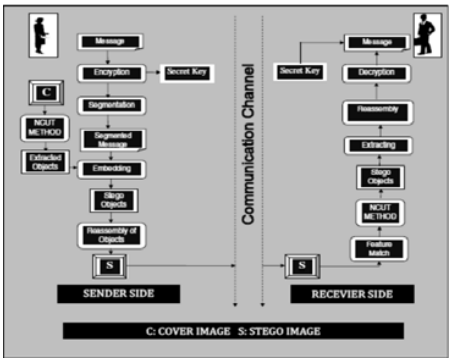

Fig. 13. Secret key steganography model

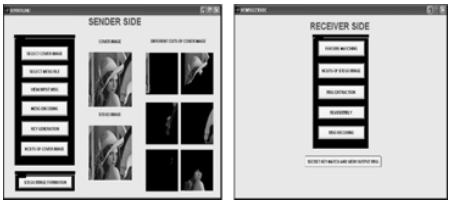

Fig. 14. GUI of the proposed model

benchmarks techniques. First one is the capacity of hiding data and another one is the imperceptibility of the stego image, also called the quality of stego image. The quality of stego-image should be acceptable by human eyes. A comparative study of the proposed steganography methods with the existing methods like PVD,GLM and the methods proposed by Ahmad T et al. has been show by computing embedding capacity, mean square error (MSE) and peak signal-to noise ratio (PSNR).The authors also compute the normalized cross correlation coefficient for computing the similarity measure between the cover image and stego image. In Fig 16 a segment of Lena as cover image has been shown. Fig 17 shows the same segment of Lena as stego image after embedding the encrypted form of the original message **"I am an Indian and I feel proud to an Indian."** on that segment. A comparison of the embedding capacity has been illustrated in figure 15.

IMAGE	IMAGE SIZE	PVD	GLM	AHMAD ET ALL.	PMM
LENA	128x128	**	2048	2493	4786
	256x256	**	8192	10007	20024
	512x512	50960	32768	40017	90680
PEPPER	128x128	**	2048	2443	5720
	256x256	**	8192	9767	23388
	512x512	50685	32768	39034	93184

Fig. 15. Comparision of embedding capacity

** For PVD method all the images used are of size 512x512.

In Fig 18 shows the image of Lena as cover and also as stego after embedding the message **"I am an Indian and I feel proud to an Indian."**.

A. Peak Signal to Noise Ratio (PSNR)

PSNR measures the quality of the image by comparing the original image or cover image with the stego-image, i.e.

41	12	122	34	123	38	64	57	56	89
12	23	74	34	53	75	49	54	67	54
75	87	91	94	97	97	94	95	97	97
96	94	95	98	97	96	97	98	93	95
20	18	24	18	18	15	16	18	13	17
76	68	55	45	29	17	20	19	14	12
90	88	87	88	85	88	88	86	85	87
78	78	79	82	78	74	72	61	64	66
83	84	89	81	81	78	67	55	38	27
91	91	95	90	87	87	90	89	90	93

Fig. 16. A Segment of Cover Image with selected pixel"

32	17	124	46	116	42	66	55	51	89
7	23	68	35	53	69	49	54	69	54
66	81	88	93	103	98	88	85	110	97
109	81	80	104	103	98	109	101	86	95
21	18		21	18	7	21	18	7	17
64	69	48	36	21	31	22	23	15	12
86	87	88	83	81	80	80	80	80	87
69	78	68	85	78	67	66	61	71	66
93	87	88	88	87	66	74	53	35	27
91	91	95	90	87	87	90	89	90	93

Fig. 17. The same segment of Stego Image with selected pixel with the embedded msg segment "I am an Indian, India is my country"

Fig. 18. A) Cover Image B) Stego Image of Lena after embedding "I am an Indian and I feel proud to an Indian."

it measures the percentage of the stego data to the image percentage. The PSNR is used to evaluate the quality of the stego-image after embedding the secret message in the cover. Assume a cover image C(i,j) that contains N by N pixels and a stego image S(i,j) where S is generated by embedding / mapping the message bit stream. Mean squared error (MSE) of the stego image as follows:

$$MSE = \frac{1}{[N \times N]^2} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(ij) - S(ij)]^2$$

The PSNR is computed using the following formulae:

$$PSNR = 10 \log_{10} 255^2 / \ MSE \ db.$$

A comparative study of PSNR of various methods has been illustrated in figure 19.

B. Similarity Measure

For comparing the similarity between cover image and the stego image, the normalized cross correlation coefficient (r) has been computed. In statistics, correlation indicates the strength and direction of a linear relationship between two random variables. The correlation coefficient ρ_{xy} between two

IMAGE	IMAGE SIZE	PVD	GLM	AHMAD ET ALL	PMM
LENA	128x128	36.20	30.5	44.30	36.5864
	256x256	35.00	33.20	46.80	36.0547
	512x512	41.79	35.50	55.00	34.7396
PEPPER	128x128	38.70	38.00	43.50	34.9404
	256x256	35.00	37.20	47.50	36.2118
	512x512	40.97	34.00	52.50	36.9247

Fig. 19. Comparison of PSNR

random variables X and Y with expected values μ_x andμ_y and standard deviations σ_x and σ_y is defined as

$$\rho_{x,y} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{E((X-\mu_x)(Y-\mu_y))}{\sigma_x \sigma_y}$$

where E is the expected value operator and cov means covariance. The value of correlation is 1 in the case of an increasing linear relationship, -1 in the case of a decreasing linear relationship, and some value in between in all other cases, indicating the degree of linear dependence between the variables.

Cross correlation is a standard method of estimating the degree to which two series are correlated. Consider two series x(i) and y(i) where i=0,1,2,. . . ,N-1. The cross correlation r at delay d is defined as

$$r = \frac{\sum_i [(x(i)-mx)(y(i-d)-my)]}{\sqrt{\sum_i (x(i)-mx)^2}\sqrt{\sum_i (y(i-d)-my)^2}}$$

where mx and my are the means of the corresponding series. The cross-correlation is used for template matching which is motivated through the following formula

$$r = \sum_{\substack{x \\ y}} f(x,y)t(x-u,y-v)$$

where f is the image and the sum is over x, y under the window containing the feature t positioned at u, v.

Similarity measure of two images can be done with the help of normalized cross correlation generated from the above concept using the following formula:

$$r = \frac{\sum_{(C(i,j)-m_1)(S(i,j)-m_2)}}{\sqrt{(\sum_{C(i,j)-m_1})^2}\sqrt{(\sum_{S(i,j)-m_2})^2}}$$

Here C is the cover image, S is the stego image,m_1 is the mean pixel value of the cover image and m_2 is the mean pixel value of stego image. It has been seen that the correlation coefficient computed here for all the images is almost one which indicates the both the cover image and stego image are of highly correlated i.e. both of these two images are same.

VII. Analysis of the Results

In this article a novel secret-key image based data hiding model has been proposed.Here the authors have used an efficient image based steganography approach (PMM) for hiding information in a gray scale image.A new approach of data encryption technique has been proposed.Comparison of PMM technique has been shown with some existing methods

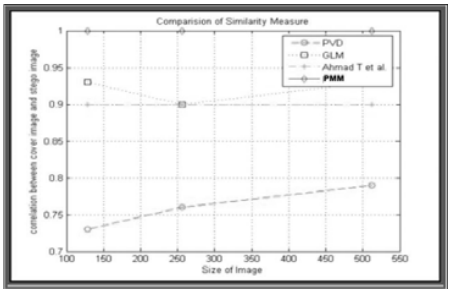

Fig. 20. Comparision of Similarity Measure for Lena

like PVD, GLM and the technique proposed by Ahmad T et al. From the experimental results in can be seen that the embedding capacity of PMM is better compared to PVD, GLM and other technique and also the similarity measures proves that the proposed method is best among these four methods which ensures that cover image and the stego image is almost identical. Also as the message bits are not directly embedded at the pixels of the cover image, steganalysis may be able to find out the embedded bits but can not be able to extract the original message bits. Besides PSNR value of the proposed method for various size of the image is much better than compared to other methods.Besides this in the previous work made by different researchers it has been seen that emphasis is given on message embedding technique to make it robust over any image processing operation. In this work an attempt has been made to increase the level of security of the steganography model by incorporating the idea of secret key, along with the use of encoded and segmented form of the original message. Further the object extraction of the cover image, formation of stego objects, assembly of stego objects to generate stego image and feature matching of stego image has also been used to increase the level of security.

The Levels of Security incorporated in the proposed model:

- Generation of the encrypted form of the secret message through sequential machine.
- Generation of secret key.
- Embedding and extraction through an efficient method (PMM).
- Segmentation of the encrypted message.
- Extraction of cuts of the cover image and generation of stego objects.
- Assembly of stego objects to form the stego image.
- Feature matching of the stego image.
- All the processes both in sender side and receiver side must be executed in proper sequence.

VIII. Conclusion

The work dealt with the techniques of a novel steganography model as related to gray scale image. A new and efficient steganographic method with high embedding capacity for embedding the secret message into image without producing any major changes has been shown here.This method also capable of extracting the secret message without the cover image. In this paper authors have used the combination of a new encryption technique through sequential machine,Embedding through

PMM and NCUT based Image Segmentation technique on raw images to obtain secure stego-image. The sequential machine has been used to generate the encrypted form of the message in order to achieve high level of security. The encrypted form of the message is embedded into the cuts of the cover image to obtain the stego-objects. This property enables the method to avoid steganalysis. The integrated approach of combining encryption through sequential machine, embedding through PMM and use of segmentation techniques through NCUT enable secure transfer of the message compared to earlier techniques.

REFERENCES

[1] Ahmad T. Al-Taani. and Abdullah M. AL-Issa. A novel steganographic method for gray-level images. *International Journal of Computer, Information, and Systems Science, and Engineering*, 3, 2009.
[2] RJ Anderson. Stretching the limits of steganography. *Information Hiding, Springer Lecture Notes in Computer Science*, 1174:39–48, 1996.
[3] Ross J. Anderson. and Fabien A.P.Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection*, 16:474–481, 1998.
[4] Souvik Bhattacharyya. and Gautam Sanyal. Study of secure steganography model. In *Proceedings of International Conference on AdvancedComputing and Communication Technologies (ICACCT-2008)*, Panipath,India, 2008.
[5] Souvik Bhattacharyya. and Gautam Sanyal. An image based steganography model for promoting global cyber security. In *Proceedings of International Conference on Systemics, Cybernetics and Informatics*, Hyderabad,India, 2009.
[6] Souvik Bhattacharyya. and Gautam Sanyal. Implementation and design of an image based steganographic model. In *Proceedings of IEEE International Advance Computing Conference*, Patiala ,India, 2009.
[7] Souvik Bhattacharyya. and Gautam Sanyal. Hiding data in images using pixel mapping method (pmm). In *Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer Engineering, and Applied Computing(WorldComp 2010)*, LasVegas,USA, July 12-15,2010.
[8] J.Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36:1583–1595, 2003.
[9] C.K. Chan. and L. M.Cheng. Hiding data in images by simple lsb substitution. *Pattern Recognition*, 37:469–474, 2004.
[10] Scott. Craver. On public-key steganography in the presence of an active warden. In *Proceedings of 2nd International Workshop on Information Hiding.*, pages 355–368, Portland,Oregon, USA, 1998.
[11] Potdar V.and Chang E. Gray level modification steganography for secret communication. In *IEEE International Conference on Industria lInformatics.*, pages 355–368, Berlin, Germany, 2004.
[12] Nameer N. EL-Emam. Hiding a large amount of data with high security using steganography algorithm. *Journal of Computer Science*, 3:223–232.
[13] K.R. Venugopal K.B. Raja, C.R. Chowdary and L.M. Patnaik. A secure image steganography using lsb, dct and compression techniques on raw images. In *ICISIP 2005 Third International Conference on Intelligent Sensing and Information Processing*, pages 170– 176.
[14] P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image steganography method using tri-way pixel value differencing. *Journal of Multimedia*, 3, 2008.
[15] Y. K. Lee. and L. H.Chen. High capacity image steganographic model. *IEE Proc.-Vision, Image and Signal Processing*, 147:288–294, 2000.
[16] N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. *IEEE Computer*, 16:26–34, 1998.
[17] C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm. *Pattern Recognition*, 34:671–683, 2001.
[18] J. Shi and J. Malik. Normalized cuts and image segmentation. *IEEE Trans. PAMI*, 22:888–905.
[19] J. Shi and J. Malik. Normalized cuts and image segmentation. In *Int. Conf. Computer Vision and Pattern Recognition*, San Juan, Puerto Rico, 1997.
[20] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. *Proceedings of CRYPTO.*, 83:51–67, 1984.
[21] JHP Eloff. T Mrkel. and MS Olivier. An overview of image steganography. In *Proceedings of the fifth annual Information Security South Africa Conference.*, 2005.
[22] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24:1613–1626, 2003.
[23] Y.K.Lee. and L.H.Chen. High capacity image steganographic model. In *IEEprocedings online no. 20000341*, 2000.

Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as a Senior Lecturer in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing.

Gautam Sanyal has received his B.E and M.Tech degree from Regional Engineering College (REC), Durgapur, now, National Institute of Technology (NIT), Durgapur, West Bengal, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, West Bengal, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 40 research papers in International and National Journals / Conferences. His current research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Student's Welfare) at National Institute of Technology, Durgapur, West Bengal, India.