High Capacity Steganography Protected using Shamir's threshold scheme and Permutation Framework

Sanjive Tyagi, Rakesh Kumar Dwivedi, Ashendra Kumar Saxena

***Abstract*: This paper presents a framework that conceal large volume of secret information using distributed file system that permit implantation of decomposed secret images across multiple-cover images. The strong security is imposed utilizing Shamir's threshold scheme and permutation generator framework. Three layers of security is being applied to protect the secret information, in first, secret image is decomposed into equal size of smaller sub-images and generate a framework of permutations from an integer for distributing and reassembling the circulated broken secret sub images among the intended participants. At the time of embedding purpose of permutation generator is to shuffle the sub-images in unknown order for outsider. During the discloser stage only inverse of permutation can rearrange the distributed sub-images to reassemble into original image by authorized contributors. In second, Shamir's threshold scheme is designed for authentication of shared associated stego-cover images before starting the extraction process. This process provides an extremely secured construction of shared secret information. In third, image is divided in 2x2 blocks of pixels and traverses it in zig-zag manner; the pixel value difference is computed for all Red, Green, and Blue (RGB) components between non-overlapping pixels of selected diagonal path with in targeted block. Secret bits are concealed inside RGB color pixels of cover image by utilizing proposed novel pixel-value differencing (PVD) scheme, furthermore varying embedding capacity may be obtained by controlling the selection of number of 2x2 block. Exploratory result displays that the proposed approach provides productive algorithms in term multilayer unbreakable security and higher payload of embedded information.**

***Index Terms*: Secret sharing, Distributed steganography, Pixel value differencing, Cryptography.**

I. INTRODUCTION

. Security is a fundamental part wherever in our life to keep the data ensured with the target that any unapproved could not take them. Consequently, there is an earnest interest for a safe communication of confidential information through the Internet. Thus, various information security strategies have been conceived to ensure the confidentiality of digital information like password protection, finger-printing protection, eye-lock protection, secret key, etc. However, today in global digital communication, activities like unlawful accessing, tempering, and breaking the copyright act are increasing tremendously, and in addition information on open network channel might be purposefully tempered by some rival who attempts to stop the information from being effectively sent or received. Therefore, there is a need to guarantee to protect confidential information by using digital security methodologies which can be cultivated by covering up secret digital information inside another digital file or by changing it into a non-understandable model. As such, steganography and cryptography developments can be expected an imperative part in digital data security structure. Cryptography has its own centrality to protect the secret data by making non-understandable. In this way, its shortcoming is encryption data can make the suspicious about its security and can be tempered by the outsider however favored point of view of steganography is, it protects the secret data by implanting it into another digital file covertly, so making the secret data subtle so there is less probability of vulnerability. Steganography is an emerging research field keeping the objective to give best in advancement of information security structure [1].

Pixel-Value Differencing (PVD) method was introduced by author in [2] to embed confidential data within gray valued images. Proposed technique trusts on the possibility that entire pixels cannot be utilized to embed to similar number of confidential bits. There are some chosen pixels which can be used to embed a greater number of pixel bits without affecting visual quality whereas some pixels can hide only less number secret bits for the reason if a greater number of bits are embedded then visual quality affects. In study authors found the quantity of bits to be implanted depends on the contrasts between sets of nearby pixels and also recommended that PVD technique can effectively give larger embedding limit with remarkable imperceptibility of stego-image. This approach partitions the cover image into non-overlapping squares containing two interfacing pixels and changes the pixel contrast in each square for implanting the secret data. PVD is planned such a way that pixel alteration does not disturb visual quality of gray scale images and 24-bits red, green and blue (RGB) color images as per the attributes of human vision affectability.

A technique of PVD checks the cover image from the upper-left corner in crisscross and partitions it into blocks with two adjacent non-overlapping pixels in each square. Quantity of bits to be embedded is determined by properties of smoothness and contrast of cover image. A smoothness and contrast property of the cover image is classified on the basis of difference value of two-pixel blocks. In the edge region pixel-value difference is substantially larger

Revised Manuscript Received on June 15, 2019.

Sanjive Tyagi, *College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, India*.

Rakesh Kumar Dwivedi, *College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, India*.

Ashendra K. Saxena, *College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, India*.

whereas smooth area has little differences. The bigger the PVD the more bits to be embedded covertly.

In [3] author suggested steganography scheme in which approved sender implants the secret image with the assistance of a group of n members and produces n stego-images from n carrier images having a similar size and similar number of pixels. Downside of this plan is recreation of confidential image, that is feasible just when all n members gives their n virtual images with reliability, if not extraction of secret image is beyond the imagination. However, our proposed strategy relay on triple security system.

A multi-pixel differencing scheme was suggested by [4] in which a block of four pixels is being used to compute number bits to be embedded based on three-pixel value differencing. In [5], the author suggested a multi-pixel value differencing image steganography based on LSB (least-significant-bit) substitution. Two enhanced version of pixel-value differencing (PVD) methods suggested by [6] that employing with block-based hiding technique. In [7], the author suggested LSB (least-significant-bit) substitution within four-pixel block. In [8], author presented steganography scheme based on pixel-value differencing of multimedia images.

In order to build high concealing capacity, a pixel-value differencing (PVD) strategy suggested by author in [9] that employing three-pixel sets, which are shaped evenly, vertically, and corner to corner in 2x2 square pixels. The estimation of other pair is balanced by keeping up the distinction between the values of pair of pixels by utilizing the reference pair. In order to improve concealing limit, the author [10] presented PVD based steganography combined with LSB scheme that utilizing square of 2 x 2 pixels. The work presented in [11] introduces an extension of Five Pixel Pair Differencing (FPPD) steganography [12] scheme that permits to communicate multiple type of secret information by embedding across various cover images. A modulus function is being used to control beginning, end and type of secret data.

II. RELATED WORK

. The work presented in [13] introduces a strategy to share one confidential image across multiple shadow images which provides better process of storage, communication, and concealing. This approach is needed to address the issue like verification of received stego-shadow images and no approach is planned to reassemble the shared image in original structure. An approach in [14] described that distributed image steganographic scheme implants secret contents within multiple career images by utilizing Block-DCT (Discrete Cosine Transformation). In this method estimated hidden image is extracted which is not look like original hidden image. In [15] author presented a steganography approach based on DWT in which more than one secret image are embedded in one cover image. In [16], presented high capacity LSB based steganography utilizing distributed approach making stego-images stronger against several steganalysis attacks as decomposed secret information are equitably distributed among various cover images file making it harder to decide its reality, however this approach does not use appropriate scheme to reassemble circulated images.

An approach in [17] presented a steganography construction on the basis of inter-block difference with the application of eight-queen's solutions. The inter-block difference between XORED and ASCII code of secret data is being used furthermore this difference value is implanted in least significant position (LSB) covertly. Rearranging the solution of eight queen's problem offers additional security to secret information. An approach of image steganography presented by [18] utilizing a pixel mapping scheme with eight queen's solution. Besides, solution of eight queen's problem is determined by randomized approach which make more secured to confidential information. In [19], author suggested secret data distribution scheme for n number of participants. In this approach at the time of extraction, extracted secret data from less than n recipients cannot be reconstructed the fractional secret data. Size of shared secret images should be same; this is limitation of suggested scheme. The scheme presented in [20], introduces the PVD steganography in which secret bits are embedded into a pair of pixels, denoted by pixel and pixel+1. A mathematical computation is being done on 7th bit of pixel to determine next target pixel+1 every time. For the analysis of sickness and treatment by the doctor, loads of data have been shared over open and private channels. The method in [21] examines the issue and gives the arrangement of security thinking about significant viewpoints, utilizing visual cryptography for sharing distributed patient data across the private and public channels. In [22], the author implemented Shamir's secret sharing scheme to design a lossless approach for safe distribution of patient's health related images. The proposed plan exploits the repetition in ordinary medical pictures to decrease share sizes, and thus encourage loading and sharing. The proposed plan on [23] joins polynomial based secret image sharing and visual cryptography approach together, to offer stacking-to-see decoding and lossless picture remaking. In order to construct color shares, a color share generation algorithm with data embedding process is being suggested. The work presented in [24] introduces the steganography strategy that incorporates the possibility of pixel marker with varieties of two normal steganography schemes, known as pixel-value differencing (PVD) and least-significant bit (LSB). In [25], author presented hashing technique using quadratic probing that can be useful in mapping secret bits.

In conventional image steganographic methods, one secret image is implanted covertly in single carrier medium which leads to susceptibility for steganalysis attack. Furthermore, if this single stego-carrier medium leads to steganalysis attack, then whole secret information is being lost. To overcome this issue Distributed Secret Information Steganography (DSIS) is being introduced with multi security system using Shamir's threshold scheme and permutation framework. Smaller shares encourage capacity and transmission, and subsequently improve the nature of stego-images in the event that a steganography strategy is utilized for undetected transmission of secret packets between the sender and the recipient members. The Distributed Secret Information Steganography (DSIS) is being developed as a part of this proposed paper to conceal larger secret information across multiple carrier file without affecting the visual quality.

III. PROPOSED STEGANOGRAPHY TECHNIQUE

In this section, multiple strategies associated with the proposed steganographic system are discussed shown in Fig 1. The purpose of this paper is to design PVD based distributed steganography along multilayer security processes.

Our proposed approach mainly emphasis on three cases to obtain the robust PVD based image steganography with higher pay load and Distributed Secret Information Steganography (DSIS) with multi-fold security system. The first case is that, usually steganography extracts embedded information from every block of pixels, expecting information are covered up in all targeted pixels. In the event that the confidential information is adequately small, it is embedded only in a section of pixels within cover-image. While in our proposed scheme, size of embedded secret bits and type of embedded file is stored in stego-cover file so that extraction process should not traverse all pixels' block of stego-cover file. It improves the time complexity of extraction algorithm. The second case is that if secret information is adequately large, the concealing limit of a single cover image may not be sufficient to accommodate it. Then, such large secret images are decomposed into a set of equally smaller size sub-images and distribute the secret sub-images across multiple cover images using proposed PVD based steganography. The third case is that, in order to distribute sub-images are denoted by specific code obtained from proposed framework of permutation generator at the time of embedding and reassembling is being achieved by obtaining the reverse of permutation at the time of extraction. Additionally, Shamir's threshold scheme is implemented to validate the shared stego-cover image file before beginning the extraction procedure. Our innovative technique performs better than various existing steganographic PVD schemes in terms of exceptionally higher payload and Shamir's unbreakable security is being implemented, additionally it performs well in opposing the steganalysis attack because of strong security system is being introduced.

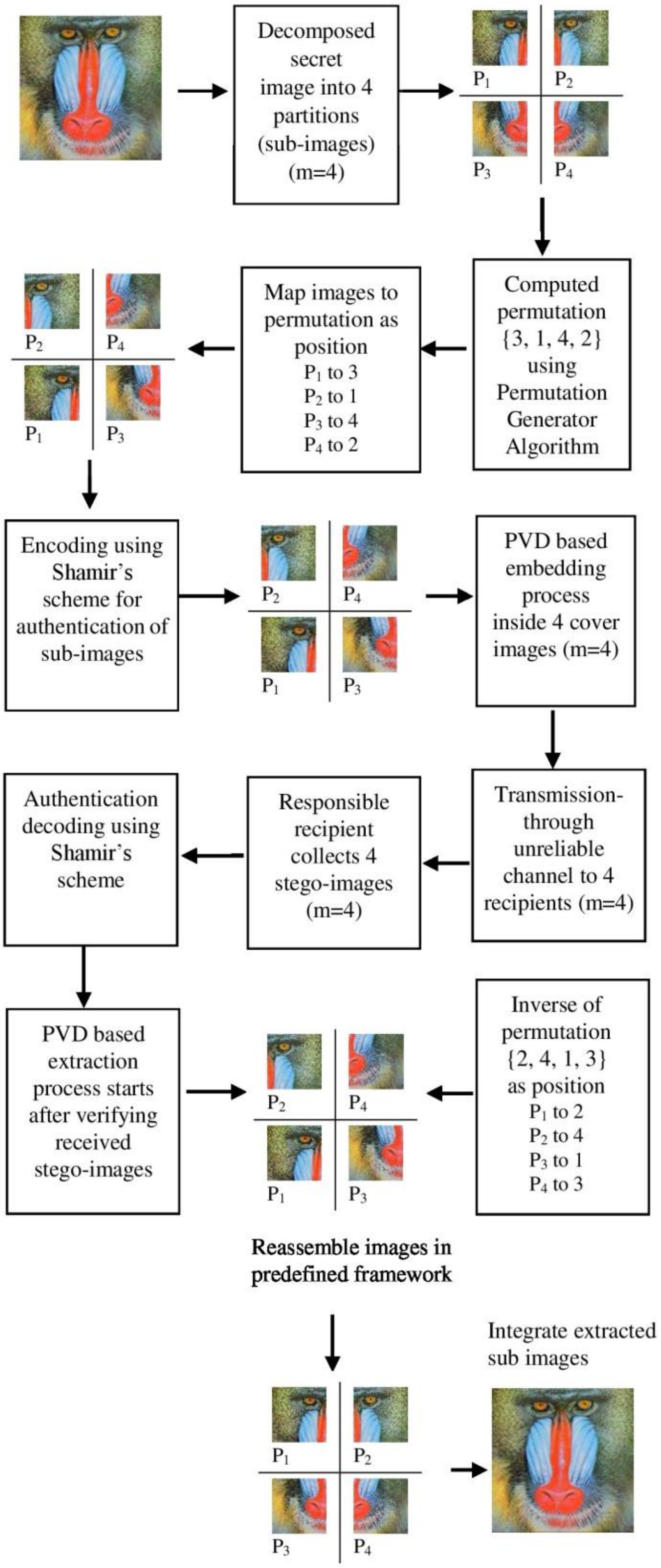
In proposed approach larger size secret image is decomposed into equal size of n sub-images and conceals them by utilizing a framework of permutation for distribution at the time of embedding and integration after the extraction, where extraction takes place after Shamir's authentication.

A. Secret Image Distributing Scheme

This section briefly discusses the secret image sharing scheme among m no. of participants.

Keeping in mind the goal to improve the amount of secret information to be concealed, the dealer at sender side is responsible to decomposed secret information S into set of m partitions as S = {S_1, S_2, S_3,… ,S_i… ..S_m} and share these partitioned images among m number of recipients as R= {r_1, r_2, r_3,… ,r_i,...,r_m} so that dealer at recipient with all m shares can reassembled the original image, whereas m-1 shares cannot extract any information about actual image. In order to hide a partitioned set S of secret images required m cover image files C= {c_1, c_2, c_3, …., c_i,… ..c_m}, and afterwards set S is implanted covertly into set C and produces the stego-cover image files SC = {sc_1, sc_2, sc_3,..… sc_i,… .sc_m}. Shamir's threshold scheme has been applied for authentication of stego-cover files to approve the received share i.e. stego-cover file by authorized recipient

Figure 1. Schematic diagram of proposed data hiding methodology


Decomposed secret image into 4 partitions (sub-images) (m=4)
P1
P2
P3
P4
Computed permutation {3, 1, 4, 2} using Permutation Generator Algorithm
Map images to permutation as position
P1 to 3
P2 to 1
P3 to 4
P4 to 2
P2
P4
P1
P3
Encoding using Shamir's scheme for authentication of sub-images
P2
P4
P1
P3
PVD based embedding process inside 4 cover images (m=4)
Transmission-through unreliable channel to 4 recipients (m=4)
Responsible recipient collects 4 stego-images (m=4)
Authentication decoding using Shamir's scheme
PVD based extraction process starts after verifying received stego-images
P2
P4
P1
P3
Inverse of permutation {2, 4, 1, 3} as position
P1 to 2
P2 to 4
P3 to 1
P4 to 3
Reassemble images in predefined framework
Integrate extracted sub images
P1
P2
P3
P4

B. Framework for Image Distributing Scheme:

This subsection describes method to evenly distribute a secret image across several cover images.

In proposed approach secret image is partitioned into m number of sub-images which are denoted by its partition number and each partitioned image has to be shared by communicating to m number of recipients. Permutation-Generator algorithm (PGA) [25] generates a sequence of numbers that decides which partitioned sub-image is to be shared to which recipient and how authorized group of recipients will integrate the received extracted shares of sub-images in order to obtain single assembled original secret image.

C. Permutation Generator Algorithm

Proposed an algorithm to generate a sequence (permutation) from integer for distributing among m recipients:

Input: P_k where $P_k \in Z_p$ and m, where p is less than or equal to m!.

Output: Permutation sequence.

Consider a string variable S= [12345…m], the P_k permutation begins from {0, 1, …, m-1}

1. Determine $s_1, s_2, \ldots, s_m$ position of character in string S from $P_k - 1 = s_1(m-1)! + s_2(m-2)! + \ldots + s_m(0)!$ where $0 \le s_i \le m-i$

2. Pick up a character at s_1 position from string S

3. Repeat step 2 for $s_2, s_3 \ldots s_m$

4. Obtained character generate a permutation sequence

5. End

D. Distribute and Integrate Partitions Algorithm

Proposed algorithm is used at the time of embedding process.

Let the size of image is S KB and dimension of image i.e. width x height is I x J pixels and have to be decomposed into m partitions, where m is no. of partitions.

Input: Image, permutation sequence generated from PGA and no. of partitions m, let's take m=4.

Output: Reshuffled partitioned images as permutation sequence.

Algorithm for Distribution

1. Start

2. Determine number of image cells in partitioned matrix that is number of partitioned rows x number of partitioned columns, compute R x C, where R=number of rows and C = number columns

3. Determine image-cell-width = image-width / C

4. Determine image-cell-height = image-height / R

5. Image is decomposed into m=4 partitions of smaller dimensions, where each image is represented by P_i, 0 <i< = m

6. Create arrays partition-image[], framework[], recipient[] of size m

7. Allocate each partitioned image to partition-image array

```
        for i = 1  to m
          partition-image[i] = P_i
```

8. Create the framework of distribution or integration to array framework[m] generated from a private key using Permutation-Generator-Algorithm (PGA).

9. Create array recipient[m] for mapping the recipient list, number of recipient R_i are equal to number of partition-image P_i where 0 <i<= m

10. Mapped the partitioned images to array recipient [m] according to framework [m]

```
        for i = 1 to m
          recipient[i]= partition-image[framework[i]]
```

//partitioned image is assigned to ith recipient partitioned images are communicated to corresponding recipient at destination.

11. End

E. Algorithm for Integration

Proposed algorithm is used at the time of extraction.

Input: m number of distributed images from m number of recipients, permutation sequence based on indexing with recipient number

Output: Rearranged partitioned images in an order

1. Start

2. Collect m number of partitioned distributed images from m number of recipients

3. Create arrays reassemble-partition-image[], framework[], recipient[] of size m

4. Array recipient[] contains the mapped recipient number in a sequential order

5. Create the framework of distribution and integration to array framework[m] generated from a private key using PGA

6. Images have to be integrated by all recipients. Find the reverse of mapped partitioned images with recipient[m] using reverse-framework [m]

```
  for i= 1 to m
  reassemble-partition-image[i]=recipient[framework[i]]
```

//recipient images are assigned in reassemble order

7. Integrate the image according to the framework of array Reassemble-partition-image[i]

8. End

F. Implementation Permutation Generator Algorithm

Example to demonstrate practicability of Permutation Generator Algorithm:

Assume a private key P_k and find a sequence of distribution needed for m=4 (number partitioned images in taken case)

Let $P_k = 17 \in Z_{23}$ and here m =4 as 23 ≤ m! i.e. 24

Need to find as

$P_k - 1 = s_1 (m-1)! + s_2 (m-2)! + \ldots + s_m(0)!$ where $0 \le s_i \le m-i$ and consider string S=1234

$16 = s_1 (3)! + s_2 (2)! + s_3 (1)! + s_4 (0)!$ eq. 1

Obtain s1=2, s2=2, s3=0, s4=0 from eq. 1

Then obtain $S_1=3$, $S_2=4$, $S_3=1$, $S_4=2$, using step 2 of above algorithm

Therefore permutation used within framework of decomposed secret information S into m partitions for distribution as {S_1, S_2, S_3, S_4} is {3, 4, 1, 2}, where m is taken as 4.

Example to demonstrate concept of Algorithm for Distribution

Consider an image of Lena.jpg of 20.00 KB (color: true, type: jpeg, dimension 256 x 256 pixels) have to be partitioned into four files of type: jpeg of equal dimension as given (color: true, dimension 128x128 pixels) such that total size of four decomposed files is also 20.00 KB. Total size of split images is equal to original file Lena.jpg. Lena.jpg with dimension width x height = 256 x 256 pixels have to be split into four equal dimension smaller sub-images requires no. of rows = 2, no. of columns = 2.

- Compute m = R x C =2 x 2 = 4, where C = 2, R=2
- image-cell-width = image-width / C =256 / 2 = 128
- image-cell-height = image-height / R = 256 / 2 = 128
- Image Lena.jpg is decomposed into m = 4 partitions P_1, P_2, P_3, P_4 of smaller dimensions, where each image is represented by P_i, 0 <i< = m
- Allocate each partition image to partition-image array Example:
  - partition-image[1] = P_1
  - partition-image[2] = P_2
  - partition-image[3] = P_3
  - partition-image[4] = P_4
- Create the framework of distribution/integration obtained from -**Framework Generator Algorithm** and assigned to array framework[m]
  - framework[4]={3,4,1,2}
- Create an array recipient [4] for the shareholders recipient
- Mapped (reshuffling) the partitioned images to array recipient [4] according to framework [4] = {3, 4, 1, 2}

```
recipient[1]= partition-image[framework[1]]
recipient[1] = partition-image[3] = P3

recipient[2]= partition-image[framework[2]]
recipient[2] = partition-image[4] = P4

recipient[3]= partition-image[framework[3]]
recipient[3] = partition-image[1] = P1

recipient[4]= partition-image[framework[4]]
recipient[4] = partition-image[2] = P2
recipient[4]={3,4,1,2} // permutation obtained
```

from-Framework Generator Algorithm
Partitioned images are communicated to corresponding recipient at destination.

Example to demonstrate concept of algorithm for Integration

- Let us take m=4
- Array recipient[m] contains the mapped partitioned no. of confidential image received by recipient no.
- framework [4] = {3, 4, 1, 2}
- recipient [4] = {3, 4, 1, 2}recipient number in a sequential order
- Images have to be integrated by all recipients after extraction process. Find the reverse of mapped partitioned images from array framework[m].
- From algorithm we have

```
reassemble-partition-image [i] = recipient [framework[i]]
reassemble-partition-image [1]=recipient [framework [1]]
reassemble-partition-image [1]=recipient [3] = P1
reassemble-partition-image [2]=recipient [framework [2]]
reassemble-partition-image [2] = recipient [4] = P2
reassemble-partition-image [3]=recipient [framework [3]]
reassemble-partition-image [3]=recipient [1] = P3
reassemble-partition-image [4]=recipient [framework [4]]
reassemble-partition-image [4] = recipient [2] = P4
```

- Integrate the images according to the framework of array reassemble-partition-image [i]

G. Shamir's Threshold Scheme for Authentication Process of Stego-Cover Image Files

After embedding the distributed secret information across multiple cover images using DSIS, obtained multiple stego-cover images are communicated to authorized recipients. Here stego-cover image files are reshuffled and mapped with recipient no. by utilizing proposed permutation (PGA) scheme. During the discloser stage before starting the extraction process, authentication of stego-cover image files have to take place because file could have been altered by third party. In such condition, there is no benefit of extraction process, however if authentication process is being applied then extraction process provides appropriate and required secret information otherwise stego-cover image files are discarded and request is done for another stego-cover image file.

In proposed approach authentication methods using Shamir's threshold scheme is being introduced for secured communication. The proposed plan distributes secret images among N no. of recipients (N is equal to m) and for recuperation all N recipients are required, on the off chance that one of the recipients is missing, at that point dealer towards recipients' side could not recreate the secret information

According to Shamir's threshold scheme a secret key K is shared among N number of participants by generating individual share from secret key K for each recipient as R_i {x_i (public key), y_i (private-Stego-key)}, this private-stego-key y_i is attached with each stego-cover image that key is known to only intended recipient $R_{i,}$ where 1<=i<=N.

Consider a set of recipient R= {R1, R2, R3, R4} i.e. four participants are required if the secret information is decomposed in four parts, here number of participants can be modified according to partition process of secrets information before hiding into Cover images.

For example, If there are four recipients (N and m is equal to 4) then each recipient R_i will have private-stego-key y_i, where 1<= i<=4. Their shares are verified by computing private key K value from available shares of private-stego-key y_i by authorized recipient, if the private key K regenerated correctly that indicate all received stego-cover image files are valid otherwise request is done to resend the valid stego-cover image files.

Algorithm for Authentication

Input: Sequence of N number of recipients, root-secret-key K, m no. of stego-images, where m=N
Output: Shares generated for each recipients R_i {x_i (public key), y_i (private key)}

Step 1: Decides number of recipients based on number of stego-cover images to be protected, denoted by N=4 in taken case.
Step 2: Decide confidentially root-secret-key K, which is

to be divided among N recipients.

Step 3: Choose threshold, which is equal to N in proposed scheme.

Step 4: Suppose root-secret-key K=11, generate polynomial on the basis of threshold value

$f(x)=11+7x^1 +3.x^2 +1.x^3$, where randomly taken (N-1) numbers i.e. $a_1=7$, $a_2=3$, $a_3=1$ and secret key $a_0=11$.

Step 5: Calculates private-stego-key y_i for each recipients R_i, where 1<=i<=N, shown in Table 1 using eq. (1).

Step 6: Assign private-stego-key y_i to each Stego-cover image file

Step 7: Communicate N stego-cover image files to N recipients of authorized group, this number N is known to responsible recipient.

Step 8: Dealer of authorized group regenerate root-secret-key from N stego-key obtained from N recipients.

Dealer collects four stego-key i.e. $\{x_i$ (public-key), y_i (private-key), shown in Table 1 as R1- {1,22}, R2-{2,45}, R3-{3,86}, R4-{4,151} from four recipients and compute root-secret-key using equation 1 as shown in Table 1.

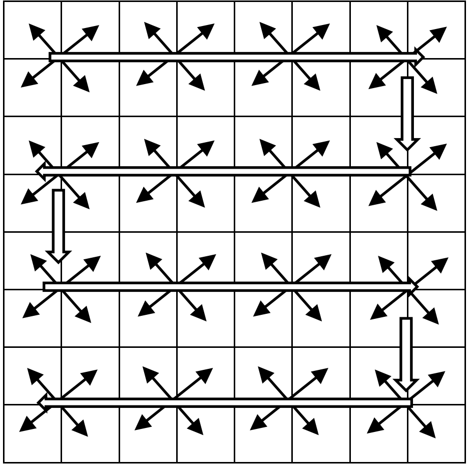
$$f(x) = \sum_{j=0}^{N} y_j \prod_{m=0,m\neq j}^{N} \frac{x - x_m}{x_j - x_m} \qquad \text{eq. (1)}$$

Step 9- if root-secret-key is valid then accept stego-cover image files and start extraction process else request is done to resend stego-cover image files.

Table 1. Authentication Process of m no of stego-cover image files (m=4) using Shamir's threshold scheme.

SN	Polynomial to produce secret shares $f(x)=11+7x^1 +3.x^2 +1.x^3$	Generate private key for 4 recipients	Recipients/ Participants	Shares generated for each recipients R_i $\{x_i$ (public key), y_i (private key)}	Interpolating polynomial
1	f(1)=11+7x1+3x1^2+1x1^3	22	R1	{1,22}	$x^3+3x^2+7x+11$ Free coefficient is required root-secret-key
2	f(2)=11+7x2+3x2^2+1x2^3	45	R2	{2,45}	
3	f(3)=11+7x3+3x3^2+1x3^3	86	R3	{3,86}	
4	f(4)=11+7x4+3x4^2+1x4^3	151	R4	{4,151}	

Figure 2. Path of targeted block into 2 x 2pixels taken diagonally cover image



H. Proposed Novel Pixel Value Differencing Method

In proposed steganography technique cover image pixels are considered in the form matrix of m x n dimension. Each cell of matrix indicates RGB pixel of 24 bits. In this, embedding process takes place in non-overlapping block of 2 x 2 pixels. Pixel Value Differencing (PVD) is computed within 2 x 2 pixels block diagonally and path within image is taken as shown in Fig 2. Proposed approach is designed with various level of embedding capacity by selecting varying positions of 2 x 2 pixels block.

Proposed innovative approach is mainly designed to keep away from smooth areas and embed secret bits just in high-intensity variation zones. The cover image is partitioned into four regions as indicated by their intensity variations. Locations with high-intensity variations case 4 embeds3 bits in each RGB components, while locations with next lower-intensity variations case 3 embeds 2 bits in each RGB components, locations with next lower-intensity variations case 2 embeds 1 bit in each RGB components and regions with variations under 9 case 1, that is, smooth regions are kept away from in the embedding procedure. Proposed algorithm traverses the embedding to the variant regions to escape statistical assaults. Notwithstanding, basic histogram analysis can recognize the discomposure of proposed methods.

The pixel value difference is computed for all Red, Green, and Blue (RGB) components between non-overlapping pixels of selected diagonal path of cover image.

Algorithm to Embed Secret Bits into Cover Image.

Input: Cover image of dimension m x n and secret image of size of dimension c x r

Output: Stego-image of dimension m x n.

Step1: For 2 x 2 block of pixel-to-edit $=P_{1,1}(R,G,B)$ to $P_{m,n}(R,G,B)$ path shown in Fig. 2, where m x n is dimension of image and m is equals to n is taken.

Step 2: Select a pair of non-overlapping pixel from across diagonal of 2 x 2 pixel block as shown in Fig. 2.

Step 3: Compute pixel value difference d_k for each RGB component between pair $P_{i,j}(R,G,B)$ and $P_{i+1,j+1}(R,G,B)$ and pair $P_{i,j+1}(R,G,B)$ and $P_{i+1,j}(R,G,B)$ diagonally as path is shown in Fig. 2, where i = 1 to n and j=1 to m and k={r, g, b}.

Step 4: Secret bits are embedded using LSB technique based on pixel value difference for each RGB component. Numbers of bits to be embedded are categorized into four cases as given

i. If pixel value difference d_k lies between 0 to 8 then no bit to be hidden.

ii. If pixel value difference d_k lies between 9 to 16 then one bit is to be hidden in corresponding R, G, B component.

iii. If pixel value difference d_k lies between 17 to 24 then two bits are to be hidden in corresponding R, G, B components.

iv. If pixel value difference d_k lies between 25 to 255 then three bits are to be hidden in corresponding R, G, B component.

Step 5: Select number bits to be embedded into variable Secret-Bits of image/text according to obtained case from step 4.

Step 6: Select a pair of pixels belongs to four cases obtained from step 4 in order to embed secret bit/bits and embedding process takes place individually to corresponding R, G, B components respectively as follows

i. If (Step 4: case i is true) then no bit is embedded.

ii. If (Step 4: case ii is true) then if decimal ($P_{i,j}$(R,G,B)) <= decimal($P_{i+1,j+1}$(R,G,B)) then hide three bits by embedding one bit into LSB of each $P_{i,j}$(R), $P_{i,j}$(G) ,$P_{i,j}$(B) and hide three bits by embedding one bit into LSB of each $P_{i+1,j+1}$(R), $P_{i+1,j+1}$(G) , $P_{i+1,j+1}$(B), else vice-versa, here 6 bits are hidden.

iii. If (Step 4: case iii is true) then if decimal($P_{i,j}$(R,G,B)) <= decimal($P_{i+1,j+1}$(R,G,B)) then hide six bits by embedding two bits into 2 LSBs of each $P_{i,j}$(R),$P_{i,j}$(G),$P_{i,j}$(B) and hide six bits by embedding two bits into 2 LSBs of $P_{i+1,j+1}$(R),$P_{i+1,j+1}$(G) , $P_{i+1,j+1}$(B), else vice-versa, here 12 bits are hidden.

iv. If (Step 4: case iv is true) then if decimal ($P_{i,j}$(R,G,B)) <= decimal($P_{i+1,j+1}$(R,G,B)) then hide nine bits by embedding three bits into 3 LSBs of each $P_{i,j}$(R),$P_{i,j}$(G) ,$P_{i,j}$(B) and hide nine bits by embedding three bits 3 LSBs of $P_{i+1,j+1}$(R), $P_{i+1,j+1}$(G), $P_{i+1,j+1}$(B), else vice-versa, here 18 bits are hidden.

Step 7: Compute pixel value difference d_k' of each RGB component for selected pair of embedded pixels in Step 6 then check d_k' that should be with the same range of four case of Step 4: if it does not satisfy then discard this pair of pixel for embedding.

Step 8: Repeat step1 through 8 until all pair of non-overlapping blocks on cross diagonally path is selected.

Algorithm to Extract Secret Bits from Stego-Image

Input: Stego-image of dimension m x n.

Output: Secret image of size of dimension c x r.

Step 1: For 2 X 2 block of pixel-to-edit = $P_{1,1}$(R,G,B) to $P_{m,n}$(R,G,B) path shown in Fig. 2, where m x n is dimension of image and m is equals to n is taken.

Step 2: Select a pair of non-overlapping pixel from cross diagonal of 2 x 2 pixel block as shown in Fig. 2.

Step 3: Compute pixel value difference d_k' for each RGB component between pair $P_{i,j}$(R,G,B) and $P_{i+1,j+1}$(R,G,B) and pair $P_{i,j+1}$(R,G,B) and $P_{i+1,j}$(R,G,B) diagonally as path is shown in Fig. 2, where i = 1 to n and j=1 to m and k={r, g, b}.

Step 4: Secret bits are to extracted using LSB technique based on pixel value difference for each RGB component. Numbers of bits to be extracted are categorized into four cases as given

i. If pixel value difference d_k' lies between 0 to 8 then no bit to be extracted.

ii. If pixel value difference d_k' lies between 9 to 16 then one bit is to be extracted from corresponding R, G, B component.

iii. If pixel value difference d_k' lies between 17 to 24 then two bits are to be extracted from corresponding R, G, B component.

iv. If pixel value difference d_k' lies between 25 to 255 then three bits are to be extracted from corresponding R, G, B component.

Step 5: If pixel value difference d_k' does not satisfy any four case of step 4 then discard selected pair of pixel to extract the secret bits and go to step 1.

Step 6: Store number bits to be extracted into variable No-Secret-Bits according to obtained case from step 4.

Step 7: Select a pair of pixel belongs to four cases obtained from step 4 in order to extract secret bit/bits and extracting process takes individually to corresponding R, G, B components respectively as follows

i. If (Step4: case i is true) then no bit is extracted.

ii. If (Step4: case ii is true) then if decimal ($P_{i,j}$(R,G,B)) <= decimal($P_{i+1,j+1}$(R,G,B)) then extract three bits by taking one bit from LSB of each $P_{i,j}$(R), $P_{i,j}$(G) , $P_{i,j}$(B) and extract next three bits by taking one bit from LSB of each $P_{i+1,j+1}$(R), $P_{i+1,j+1}$(G) , $P_{i+1,j+1}$(B), else vice-versa, here 6 bits are extracted.

iii. If (Step 4: case iii is true) then if decimal($P_{i,j}$(R,G,B)) <= decimal($P_{i+1,j+1}$(R,G,B)) then extract six bits by taking two bits from 2 LSBs of each $P_{i,j}$(R), $P_{i,j}$(G) , $P_{i,j}$(B) and extract next six bits by taking two bits from 2 LSBs of each $P_{i+1,j+1}$(R), $P_{i+1,j+1}$(G) , $P_{i+1,j+1}$(B), else vice-versa, here 12 bits are extracted.

iv. If (Step 4: case iv is true) then if decimal ($P_{i,j}$(R,G,B)) <= decimal($P_{i+1,j+1}$(R,G,B)) then extract nine bits by taking three bits from 3 LSBs of each $P_{i,j}$(R), $P_{i,j}$(G) , $P_{i,j}$(B) and extract next nine bits by taking three bits from 3 LSBs of each $P_{i+1,j+1}$(R), $P_{i+1,j+1}$(G) , $P_{i+1,j+1}$(B), else vice-versa, here 18 bits are extracted.

Step 8: Arrange secret bits into eight bits/twenty-four bits in order to construct one character/one image pixel of secret data.

Step 9: Repeat step 1 through 8 until all pair of non-overlapping blocks are selected on across diagonally path for extraction process //end for step 1

Algorithms are designed to achieve innovative PVD based steganography without affecting the visual appearance of stego-image.

Table 2. PSNR and Embedding capacity of different experimented images

SN	File Name	Image	File Size in KB	Target pixel block position used	Embedding capacity in bits	PSNR	ER
1	lina.png	512 x 512 (24 bits)	462.73	All pixel position blocks	1572864.00	50.1106	5.87
				Odd pixel position blocks	786432.00	53.5116	2.89
				Even pixel positions	786432.00	53.5116	2.89
				Multiple of 4th position blocks	393216.00	56.7432	1.48
2	airplane.bmp	512 x 512 (24 bits)	768.05	All pixel position blocks	1572864.00	50.3287	5.87
				Odd pixel position blocks	786432.00	53.2280	2.89
				Even pixel positions	786432.00	53.2280	2.89
				Multiple of 4th position blocks	393216.00	57.1064	1.48
3	peppers.png	512 x 512 (24 bits)	526.12	All pixel position blocks	1572864.00	55.3342	5.87
				Odd pixel position blocks	786432.00	56.8328	2.89
				Even pixel positions	786432.00	56.8328	2.89
				Multiple of 4th position blocks	393216.00	58.2619	1.48
4	baboon.png	512 x 512 (24 bits)	622.26	All pixel position blocks	1572864.00	53.6577	5.87
				Odd pixel position blocks	786432.00	57.1874	2.89
				Even pixel positions	786432.00	57.1874	2.89
				Multiple of 4th position blocks	393216.00	59.1321	1.48

Figure 3.Embedding capacity managed by selecting varying positions of target pixel block (2 x 2) of cover image

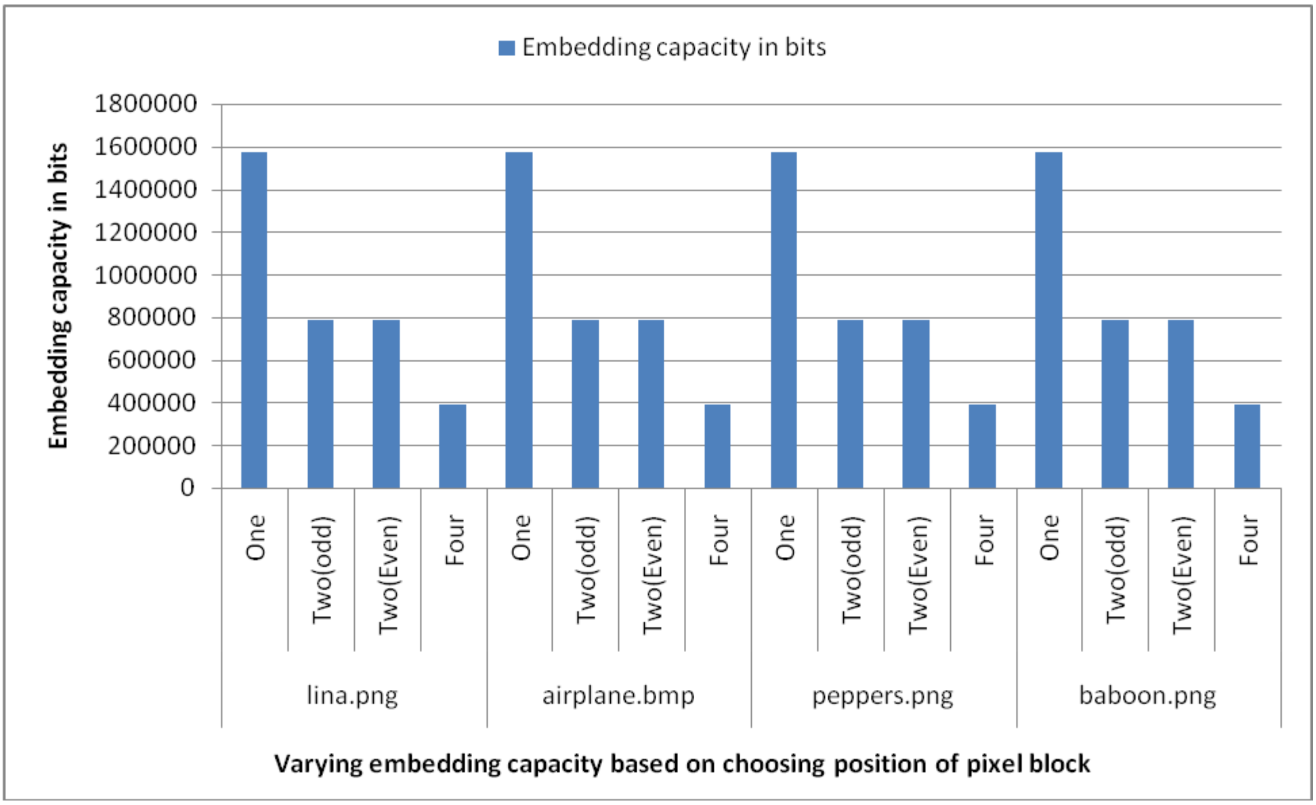
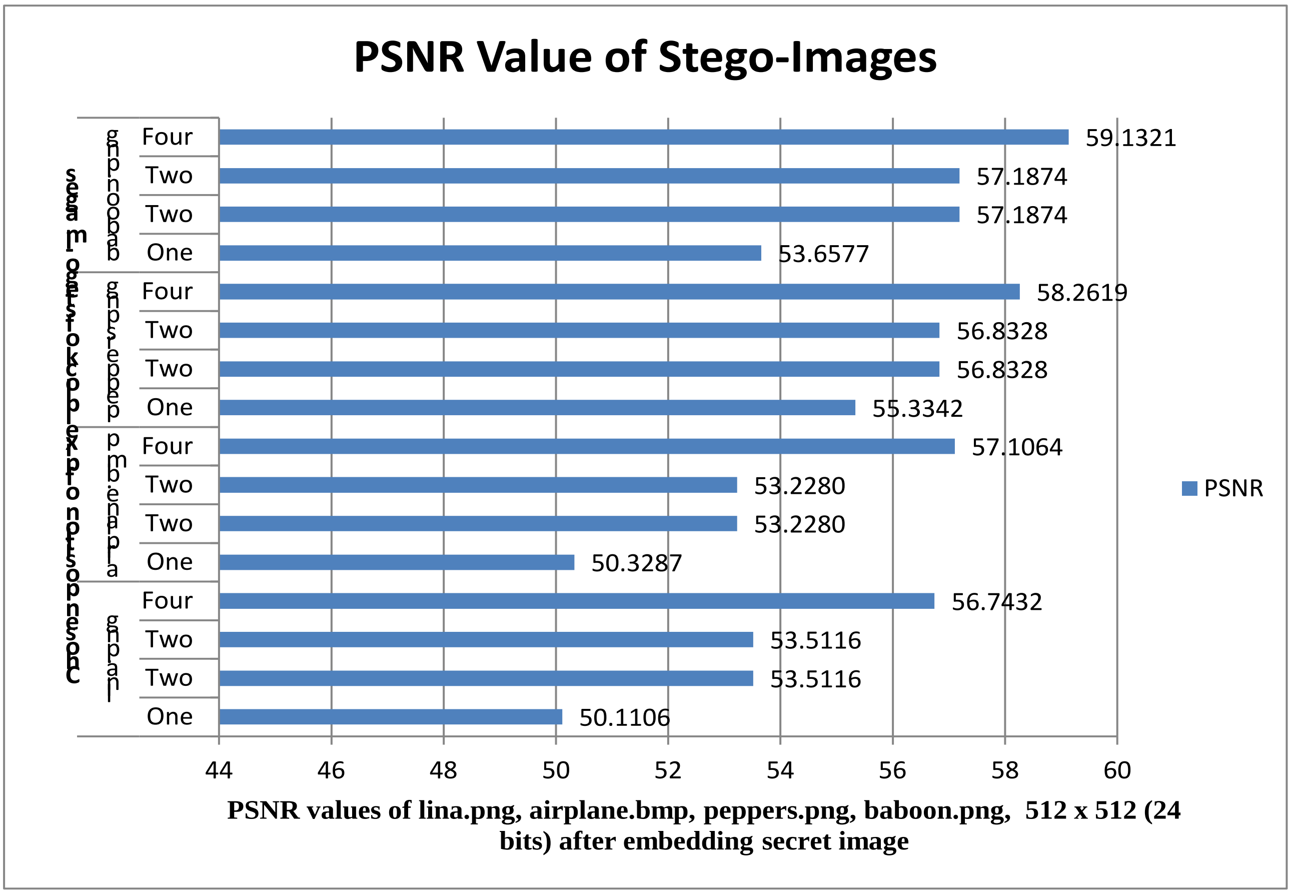


Figure 4. The signal-to-noise ratio (PSNR) values are evaluated to estimate the visual quality of stego-image



IV. RESULTS AND DISCUSSION

Here we are analyzing the performance of our proposed PVD based algorithm by utilizing various images of PNG and BMP formats.

PSNR is defined as

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right) \qquad \mathrm{eq.}\,(2)$$

MSE denotes Mean Square Error given as:

$$\mathrm{MSE} = \frac{1}{\mathrm{m\,n}}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad \mathrm{eq.}\,(3)$$

where MAX is generally maximum amplitude of the signal or simply 255 (for 8 bit data representation 2^8 -1), i and j represents the image coordinates, m and n are dimensions of the image and I(i, j) is generated stego-image (stego-image) and K(i, j) is the cover image (original image). If PSNR value is less than 30dB, then distortion due to embedding else less chances of distortion. If PSNR value is greater than 40dB, then high visual quality image is being considered.

Embedding rate is used to represent the percentage of the embedded bits of confidential image inside the cover image pixel area. The ER is characterized as in eq.(4)

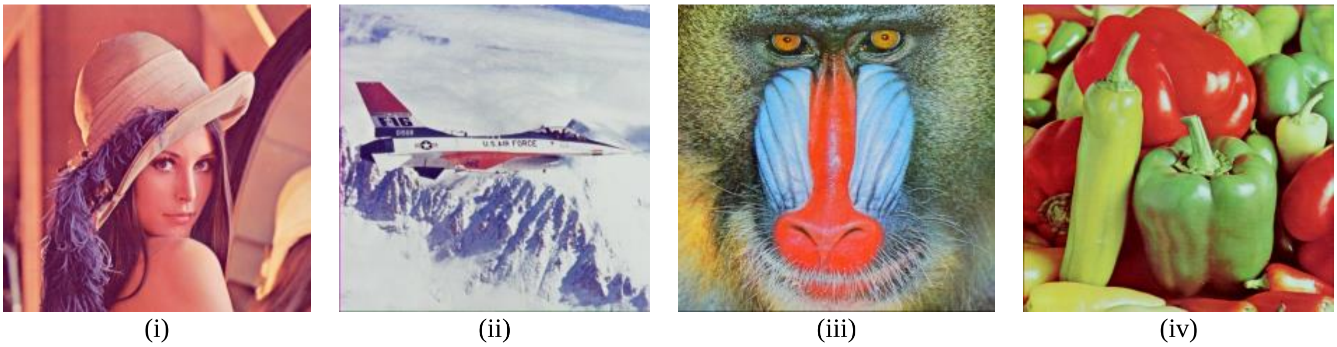
$$\mathrm{ER} = \frac{\text{Number of secret bits}}{\mathrm{m\ x\ n}} \text{ Bits Per Pixel (bpp)} \quad \mathrm{eq.}\,(4)$$

where m and n are dimension of cover image.

As indicated by the embedding capacity assessment, a higher estimation of ER indicates that approach has better execution as far as the embedding capacity, that is, a carrier image can hold additional confidential bits. However, a small estimation of ER indicates inferior performance.

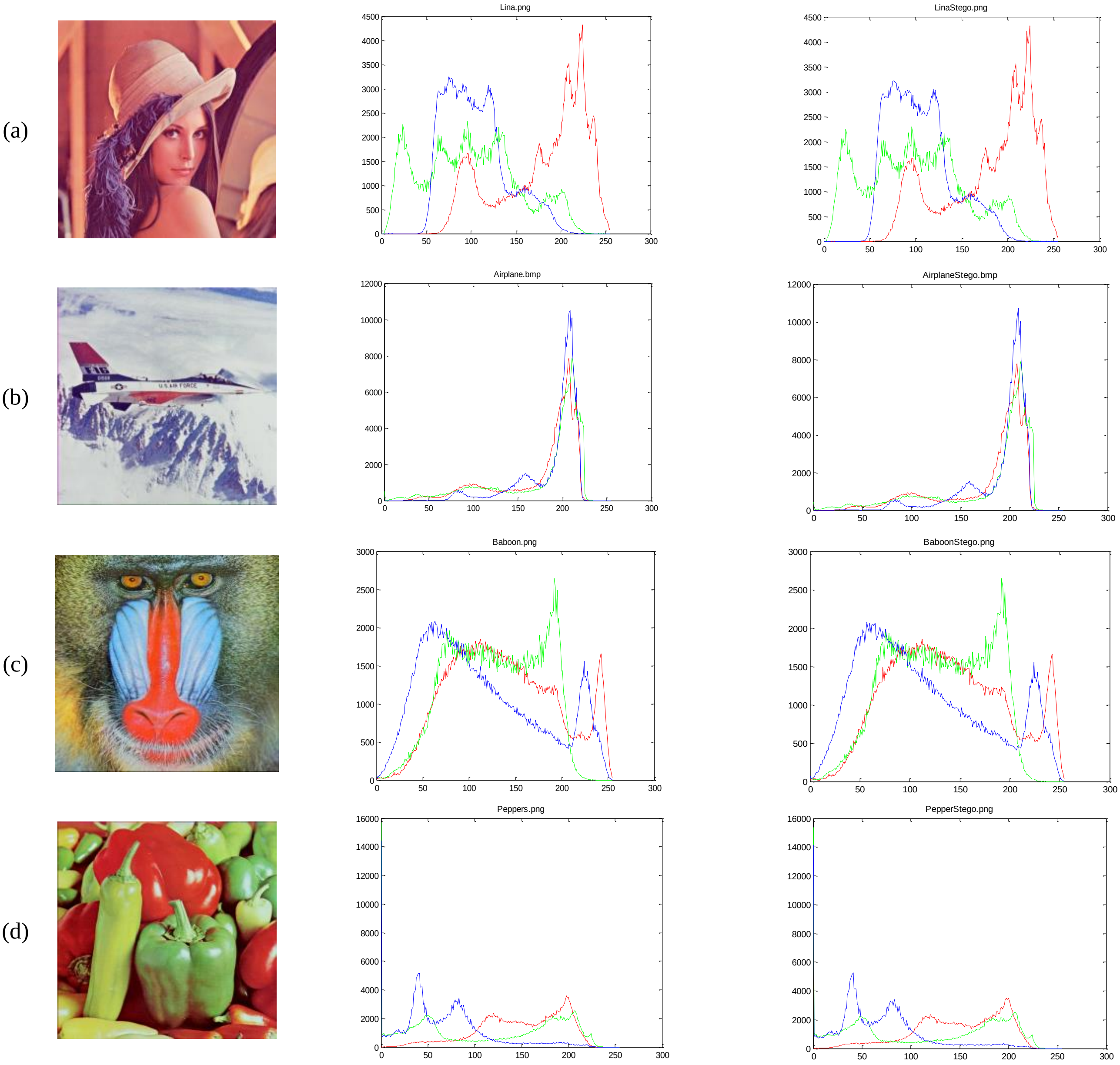
Practical implication is being done by developing a software tool SteganoPixTrans. This tool is integrated software developed on NetBeans IDE 8.2 in Java. We have experimented proposed PVD based algorithm on SteganoPixTrans tool with different images shown in Fig. 5. Results of experiential analysis are being exhibited by inspecting and validating the proposed PVD based approach in Table 2. Histograms of experimental images and PSNR values have been evaluated using MATLAB 9.0.

Figure 5. Stego-images (i) Lena.png (ii) airplane.bmp (iii) Baboon.png (iii) Peppers.png



(i) (ii) (iii) (iv)

Figure 6. Histograms of red, green and blue components for cover images and stego-images



V. ANALYSIS AND DISCUSSION

Analysis of proposed approach is being done in three phases, first is PVD based strganography, in proposed approach, a two-dimensional image is denoted in the form matrix. Here it is being observed that varying embedding capacities can be achieved by selecting varying position of targeted pixel block shown in Table 2 and Fig. 3. It is estimated that normal (typical) embedding bit rate 1.48 bpp is obtained by choosing each fourth position block, medium embedding bit rate 2.89 bpp is obtained by choosing each second position block in odd or even order and higher embedding bit rate 5.87 bpp is obtained by choosing each block of cover image as shown in Table 2. The signal-to-noise ratio (PSNR) is evaluated to estimate the visual quality of stego-image shown in Table 2 and Fig. 4; it is sufficiently higher in all four cases to satisfy our proposed algorithm. Further analysis of difference in visual quality of cover-image and stego-image is exhibited by histograms for red, green, blue components depicted in Fig. 6(a-d) that evaluate resemblance among the original cover-image and stego-image. During the study it is found that difference level between histogram of cover-images and stego-images convincingly insignificant. Henceforth, in the proposed plan, the evaluated PSNR standards just as the visual appearance of the stego-image and histogram recommend that the deviation showing up in the wake of implanting of the secret image inside the cover image is sensibly less and unnoticeable to human visual recognition.

Multi-fold security is being achieved using Distributed Secret Information Steganography (DSIS) with proposed Shamir’s authentication scheme and permutation generator algorithm (PGA). Framework of distributing of sub-images and reassembling of original image is being obtained by unique permutation generator technique. Proposed strategy conceal decomposed sub-images within multiple cover images improves embedding capacity and making it more difficult to trace than traditional steganographic methods, and mandatory to reassemble the original image from collection of affected stego-images for the retrieval of original secret image. Exploratory outcome shows that the proposed methodology gives productive strategies and algorithms in term multilayer unbreakable security, and higher payload of hidden data.

VI. CONCLUSION

High Capacity Steganography protected using Shamir’s threshold scheme and permutation framework, a novel scheme is presented in this paper. Motivating characteristic of proposed PVD based steganography approach is that embedding limit can be controlled by manipulating positions of targeted pixel block. In light of our results, we believe that sufficient high embedding bit rate 2.89 bpp may be achieved by focusing on second pixel block.

The process of distributing of secret image make it more significant because this makes the transporter image progressively resistant to different steganalysis assaults as the decomposed secret information are reshuffled at the time of distribution amongst shareholders using permutation generator. During the discloser phase just inverse of permutation can reorganize the distributed sub-images to reassemble the original image by authorized contributor. Furthermore, approved recipient ought to get n no. of stego-images, solid purpose of our innovative approach is that responsible recipient cannot reproduce the secret image until all n valid stego-images are gathered; this number n is regenerated from stego-image received by responsible contributor. In that way, through the contribution of this intended recipient only, n sub-images are extracted and consolidating all n sub-images in a deliberate manner obtained from permutation generator to reconstruct original confidential image. Shamir's threshold is being applied for validation of shared associated stego-cover images before beginning the extraction procedure. This procedure gives enormously secured reconstruction of shared secret image The experimental examination and result assessment demonstrate that introduced steganographic framework is highly secured with higher payloads, and adequate imperceptibility for stego-image. This innovative approach is practically feasible.

REFERENCES

1. S. Tyagi, R. K. Dwivedi, and A. K. Saxena, "A Novel PDF Steganography Optimized Using Segmentation Technique," International Journal of Information Technology, https://doi.org/10.1007/s41870-019-00309-7, Springer, pp 1-9, 2019.
2. D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24(9-10), pp. 1613–1626, 2003.
3. C.-C. Chang and R.-J. Hwang, “A New Scheme to Protect Confidential Images,” Journal of Interconnection Networks, Vol. 5, no. 3, pp. 221-232, 2004.
4. C. H. Yang and C. Y. Weng, “A steganographic method for digital images by multi-pixel differencing,” in *Proceedings of International Computer Symposium*, pp. 831–836, Taipei, Taiwan, 2006.
5. K.-H. Jung, K.-J. Ha, and K.-Y. Yoo, “Image data hiding method based on multi-pixel differencing and LSB substitution methods,” in *Proceedings of International Conference on Convergence and Hybrid Information Technology (ICHIT 08)*, pp. 355–358, 2008.
6. J.-C. Liu and M.-H. Shih, “Generalizations of pixel-value differencing steganography for data hiding in images,” *Fundament- Informaticae*, vol. 83, no. 3, pp. 319–335, 2008.
7. X. Liao, Q.-Y. Wen, and J. Zhang, “A Steganographic Method for Digital Images with Four-Pixel Differencing and Modified LSB Substitution,” *Journal of Visual Communication and Image Representation*, vol. 22, no. 1, pp. 1–8, 2011.
8. C.-H. Yang, C.-Y. Weng, H.-K. Tso, and S.-J. Wang, “A Data Hiding Scheme using the Varieties of Pixel-Value Differencing in Multimedia Images,” *Journal of Systems and Software*, vol. 84, no. 4, pp. 669–678, 2011.
9. K.-C. Chang, P.S. Huang, T.-M. Tu, and C.-P. Chang “Adaptive Image Steganographic Scheme Based on Tri-Way Pixel-Value Differencing,” in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC 07), pp. 1165–1170, 2007.
10. X. Liao, Q.Y. Wen, S. Shi, “Distributed Steganography,” in Proceedings of Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 153-156, 2011.
11. Fendi, A. Wibisurya, and Faisal, “Distributed Steganography using Five Pixel Pair Differencing and Modulus Function,” in Proceedings of International Conference on Computer Science and Computational Intelligence, ICCSCI, Bali, Indonesia,116 (2017), pp. 334–341, 2017.
12. A.K. Gulve, M.S. Joshi, “An Image Steganography Algorithm with Five Pixel Pair Differencing and Gray Code Conversion,” International Journal of Image, Graphics and Signal Processing, Vol. 6(3), pp. 12-20, 2014.
13. C.-C. Thien, J.-C. Lin, “Secret Image Sharing,” Computers & Graphics, Vol. (26), pp. 765-770, 2002.
14. R. Koikara, D.J. Deka, M. Gogoi, and R. Das, “A Novel Distributed Image Steganography Method Based on Block-DCT,” Advanced Computer and Communication Engineering

Technology, pp. 423-435, Springer, 2015.

15. S. Hemalatha, U. D. Acharya, A. Renuka, and P.R. Kamath, "A Secure Image Steganography Technique to Hide Multiple Secret Images", in Proceedings of the Fourth International Conference on Networks and Communications, NetCom, Vol. 131, pp. 613-620, Springer, 2012.
16. S. Tyagi, A. K. Saxena, and S. Garg, "Secured High Capacity Steganography using Distribution Technique with Validity and Reliability", in Proceedings of International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, pp.109 –114, 2016.
17. V. Kumar, A. Bansal, and S. K. Muttoo, "Data Hiding Method Based on Inter-Block Difference in Eight Queens Solutions and LSB Substitution", International Journal of Information Security and Privacy, (IGI Global), Vol. 8(2), pp. 55-68, 2014.
18. A. Bansal, S. K. Muttoo, and V. Kumar, "Data Hiding Approach Based on Eight-Queens Problem and Pixel Mapping Method", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.7(5), pp.47-58, 2014.
19. M. Deshmukh, N. Nain, and M. Ahmed, "A Novel Approach for Sharing Multiple Color Images by Employing Chinese Remainder Theorem", Journal of Visual Communication and Image Representation, Vol. 49, pp. 291-302, 2017.
20. K. Joshi , S. Gill, and R. K. Yadav, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Journal of Computer Networks and Communications, Hindawi, Volume 2018, pp. 10, 2018.
21. A. Bakshi, A. K. Patel, "Secure Telemedicine using RONI Half Toned Visual Cryptography without Pixel Expansion", Journal of Information Security and Applications, 46 (2019), pp. 281–295, 2019.
22. A. Kanso, M. Ghebleh, An efficient lossless secret sharing scheme for medical images," Journal of Visual Communication and Image Representation, Elsevier, Vol. 56, pp. 245-255, 2018.
23. X. Wua, C.-N. Yang, "A Combination of Color-Black-and-White Visual Cryptography and Polynomial Based Secret Image Sharing," Journal of Visual Communication and Image Representation, Elsevier, Vol. 61, pp.74-84, 2019.
24. A. A. Al-Sadi, E.S.M. El-Alfy , "An Adaptive Steganographic Method for Color Images Based on LSB Substitution and Pixel Value Differencing," in Proceedings of (ACC 2011) Communications in Computer and Information Science, Vol . (191), Springer.
25. https://en.wikipedia.org/wiki/Permutation
26. S. Tyagi, R. K. Dwivedi, and A. K. Saxena, "A High Capacity PDF Text Steganography Technique Based on Hashing Using Quadratic Probing", International Journal of Intelligent Engineering and Systems , Vol.12, No.3, pp. 192-202, 2019.

AUTHORS PROFILE

Sanjive Tyagi is perusing Ph.D. in Computer Application from Teerthanker Mahaveer University (TMU), Moradabad, India. He has done M.Tech. (CSE) in 2007, MCA in 2003 from MDU, Rohtak and M.Sc. Physics from CCS University, Meerut. He is working as an Associate Professor in NIT, Meerut. He has 16 years of teaching experience in various colleges. He has published various research papers as- 1. A High Capacity PDF Text Steganography Technique Based on Hashing Using Quadratic Probing in International Journal of Intelligent Engineering and Systems (IJIES- SCOPUS Indexed), 2019. 2. A Novel PDF Steganography Optimized Using Segmentation Technique in International Journal of Information Technology, Springer, 2019. 3. A Novel PDF based Text Steganography by Cross-Reference Coding Technique", in IEEE Conference-SMART-2017 at TMU, Moradabad. 4. Secured High Capacity Steganography using Distribution Technique with Validity and Reliability- in IEEE Conference-SMART-2016 at TMU, Moradabad and published 9 research paper on Digital Steganography in International Journal and 2 research paper on Smart Card Fraud Prevention Scheme in International Journal. He has attended various workshops, seminars and short terms courses in the area of computer science & engineering. His area of interest includes Information Hiding, Cryptography, Pattern Recognition, Algorithms Design and Data mining.

Dr. Rakesh Kumar Dwivedi is Professor and Principal in College of Computing Sciences and Information Technology at Teerthanker Mahaveer University, Moradabad, India. He has completed his Ph.D. degree in the area of Digital Image Processing from Indian Institute of Technology Roorkee. He has done his M.Tech. degree in CSE from H.B.T.I. Kanpur, Uttar Pradesh. He has 22 years teaching experience in the field of computer science & engineering. He has published various research papers as 37 papers in International Journals of high impact factor and 38 research papers in Conferences in India and Abroad. He has chaired the session in the World Congress of Computer Science and Computer Engineering Conference, 2014 at Las Vegas, USA. He has participated in 19 AICTE approved short term courses in the area of Computer Science. His research area of interest includes the soft computing; Fuzzy based Hybrid Soft Classification, Parameter Optimization, Algorithm Design and Uncertainty Reduction using Fuzzy Techniques. Projects & Consultancy Projects includes In-house software development. His teaching & research areas includes Computer Algorithm, Java Programming, Database Management System, Soft Computing, Digital Image Processing and Soft Classification.

Dr. Ashendra Kumar Saxena is Associate Professor in College of Computing Sciences and Information Technology at Teerthanker Mahaveer University, Moradabad, India. He has completed his Ph.D. from Mahatma Jyotiba Phule Rohilkhand University, Bareilly, India. He has done his master degree from Uttar Pradesh Technical University, Lucknow. He has 15 years teaching experience in the field of computer science & engineering. He has attended various workshops, seminars and short terms courses in the area of computer science & engineering. He has published various papers in national, international conferences and journals. His research area of interest includes the Optimization Techniques, Information Security, Operation Research, Algorithms Design and Cloud Computing.