International Journal of Web-Based Learning and Teaching Technologies
Volume 15 • Issue 1 • January-March 2020

Multi-Image Hiding Blind Robust RGB Steganography in Transform Domain

Diptasree Debnath, St. Thomas' College of Engineering & Technology, Kolkata, India
Emlon Ghosh, St. Thomas' College of Engineering & Technology, Kolkata, India
Barnali Gupta Banik, St' Thomas College of Engineering & Technology, Kolkata, India

ABSTRACT

Steganography is a widely-used technique for digital data hiding. Image steganography is the most popular among all other kinds of steganography. In this article, a novel key-based blind method for RGB image steganography where multiple images can be hidden simultaneously is described. The proposed method is based on Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) which provides enhanced security as well as improve the quality of the stego. Here, the cover image has been taken as RGB although the method can be implemented on grayscale images as well. The fundamental concept of visual cryptography has been utilized here in order to increase the capacity to a great extent. To make the method more robust and imperceptible, pseudo-random number sequence and a correlation coefficient have been used for embedding and the extraction of the secrets, respectively. The robustness of the method is tested against steganalysis attacks such as crop, rotate, resize, noise addition, and histogram equalization. The method has been applied on multiple sets of images and the quality of the resultant images have been analyzed through various matrices namely 'Peak Signal to Noise Ratio,' 'Structural Similarity index,' 'Structural Content,' and 'Maximum Difference.' The results obtained are very promising and have been compared with existing methods to prove its efficiency.

KEYWORDS

Data Privacy, Discrete Cosine Transforms, Discrete Wavelet Transforms, Information Security

1. INTRODUCTION

To find the meaning of Steganography, one has to reveal the Greek words – 'steganos' which means "concealed, covered or protected" and 'graphein' which means "writing". In summary, Steganography is the ancient art of concealing classified information into a cover object. The cover can be of the same format of the secret or of some other media. Whereas Cryptography is the science of encrypting the secret in such a way that to make it readable the recipient has to decrypt the secret with a proper key. The main advantage of steganography over cryptography is that the presence of secret is unknown to everyone except the intended recipient and hence it avoids the unnecessary attention as an object of being scrutinized despite of how secure the algorithm is.

The main objectives of steganography can be summarized as follows:

- Hide the secret effectively without revealing the existence of the secret
- Successful retrieve of the secret without any alteration
- Increase channel embedding capacity by engraving maximum bits possible to utilize the channel in the best possible manner

DOI: 10.4018/IJWLTT.2020010102

In a crux, intend of the proposed method is to introduce a new image steganography method which can hide multiple binary secrets in an RGB cover transforming into frequency domain. The aim is to enhance the capacity using visual cryptography and improve the security applying both DCT and DWT.

The field of steganography has been stratified into different domains according to the different types of covers because the cover can be taken as text, image, audio, video etc. In case of image steganography, the secret is embedded into the cover image. However, if the changes are directly incorporated into the cover image pixels, there is a high probability that the changes will be prone to easily detect. Therefore, the cover image is converted into frequency domain using various methods like discrete cosine transformation (DCT), discrete Fourier transformation (DFT), discrete wavelet transformation (DWT) etc. before making any alterations. Here DCT and DWT both will be discussed in detail as these two techniques are crux of the proposed method.

In addition, the fundamental concept of visual cryptography has been applied here to increase the capacity as well as to enhance the security of the confidential information. Visual cryptography is a notable encryption method which allows concealing information into images in such a way that the decryption can be performed using human vision even without the usage of a computer if and only if correct key images are overlapped. This has been discussed in section 2.1 with more details.

Furthermore, PN sequence has been used to embed the secret into the image while correlation function has been deployed to decrypt the information. The PN sequence is generated by using particular key k as the $(k+1)^{th}$ bit of the sequence is a function of k. The extraction procedure is based on the correlation between the same PN sequence used during embedding procedure and the modified pixel values. Therefore, to generate the same PN sequence in both embedding and extraction processes, key is essential. The proposed method has been thoroughly scrutinized through various standard metrics and the experimental results proves it efficacy and imperceptibility.

In this method, after applying visual cryptography to each color component of the RGB cover, DWT is applied followed by DCT and finally the secret is embedded in the mid-band region using PN sequence. For the retrieval, the reverse path has to follow.

2. LITERATURE SURVEY

Steganography is a technique of hiding secrets from the potential monitors or channels administrators so that they could not even know that a secret message is being transmitted. On the contrary, in case of cryptography, they know that a message is being sent but it is not in a readable format and hence it requires a key to decrypt the secret. This can be elucidated by a simple example: if a man who has no knowledge of ancient Egyptian languages finds a scroll written in hieroglyphics, the message is encrypted to him and he cannot understand it until he is able to decipher it. On the other hand, an elementary example of steganography would be if the message were written with invisible ink.

According to Kahn (1996), the origin of steganography is more likely to be physiological or biological. It comes from the natural instinct of animals to hide secrets such as turtles hiding their eggs in the sand or humans hiding treasures. While the term cryptography means “secret writing”, steganography means “covered or protected writing”. The first documented usage of steganography dates back to 440 BC when Greek ruler Histaeus shaved the head of his most trusted slaves to write secret messages on their head and finally when their hair grew back, the message was concealed. There are plenty of such examples of steganography lies in our history.

Now what differs age-old steganography from the modern ones is the format of the cover of the intended secrets. In earlier times, the preferable covers were human skin, or use of paper by writing in invisible ink, and many other simple or complex physical objects while modern steganography utilizes digital images, videos, audios as covers. As described by Swain and Lenka (2014), based on the choice of cover, digital steganography can be classified into three main categories which are - (i) image steganography, (ii) audio steganography and (iii) video steganography.

Image steganography, which is the main focus of this research article, can be further categorized into two groups i.e. spatial domain and frequency domain. The spatial domain of image steganography deals directly with the pixels of the cover image to hide the secret. Although there is high chance of detection of the secret while working in the spatial domain, there are some notable methods like LSB method, pixel differencing method etc. which work excellently in this domain. Zou et al. (2016) has proposed an effective method of hiding grayscale image into RGB image using LSB and RSA encryption method with enhanced capacity and security. Now there are several techniques to convert the image to frequency domain such as Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT), Discrete Wavelet Transformation (DWT) etc.

Sathisha et al. (2011) has proposed a novel covariance base method for embedding grayscale image into another grayscale image using DCT but the capacity is limited, and the quality of the images are also not up to the mark compared to other existing works. Similarly, the proposed method by Dey, Roy and Dey (2011) embeds color image into RGB color planes using DWT, but again the quality of the images is extremely poor, and capacity cannot be improved. Hemalatha et al. (2013) have described another method of color image steganography using DWT and IWT (Integer Wavelet Transformation) but again the capacity is stagnant, and quality of image degrades. Even though both methods, DCT and DWT are effective in the transform domain, when applied separately, they degrade the quality of the images in many cases. That is why this paper proposes a method where both DCT and DWT has been used which results in better quality of the image.

Rishi et al. (2011) has proposed a method to enhance the embedding capacity. The secret under consideration is a matrix of logical values which can be consider as single bits representing each pixel value of a binary image. In case of a binary image the process shows positive results. However, if one tries to embed a grayscale image for which each pixel takes 8 bits to represent, the embedding capacity decreases. Furthermore, in case of an RGB secret image which requires 24 bits to represent each pixel, the embedding capacity further deteriorates. Thus, here embedding capacity depends on the type of secret used.

Ogiela et al. (2015) has proposed a method for multiple image steganography. However, there is no improvement in embedding capacity rather two secrets or images are impeding in the capacity of one thus compromising the quality of the actual secret.

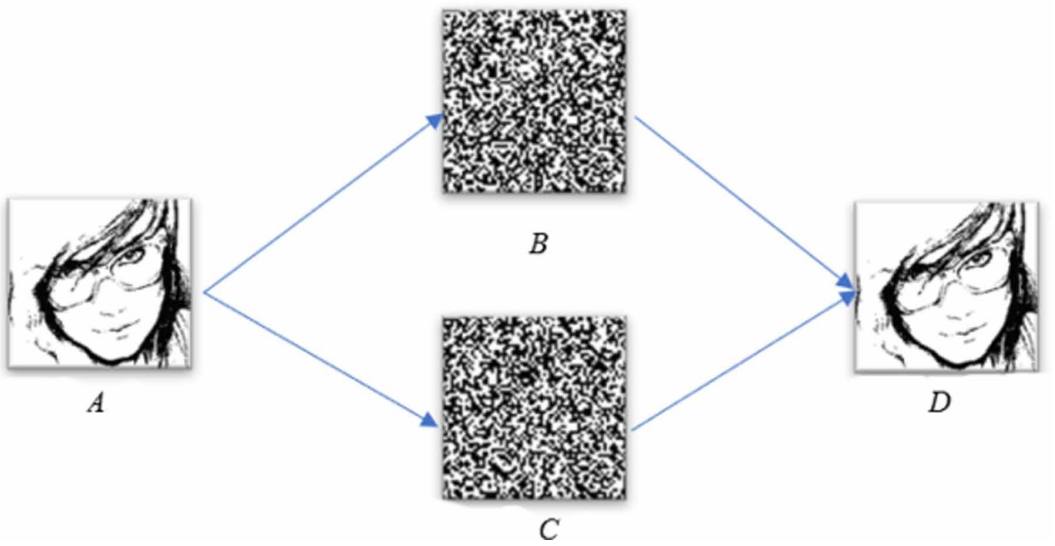
Tang et al. (2014) has proposed a new method which would have high embedding capacity by using multi-level embedding. However, the cover is a gray scale image and the most commonly used image is a colored image but there is no mention of this process's approach towards an RGB image as a cover. The embedding procedure deals with embedding bits, so the embedding capacity here also depends on the type of secret. That is why the proposed method intends to take RGB as a cover message which is the most popular means of communication in today's world and to improve the capacity, visual cryptography has been introduced.

2.1. Fundamentals Concept of Visual Cryptography

The pioneers of Visual Cryptography are considered to be Naor and Shamir (1994) who introduced a method for visual secret sharing where a secret image is divided into n number of shares and only who has all the n shares can overlap the images to find the true secret. The term 'Visual' was incorporated because no computation was required to reveal the secret, only overlapping all the shares would unfold the secret to naked human eyes. Later, Zhou et al. (2006) proposed Halftone Visual cryptography technique to enhance the quality of the retrieved secret image. As it can be shown in the figure 1 below, Figure 1A is the original secret image which has been divided into two shares (Figure 1B and 1C) and overlapping those two shares regenerates the secret (Figure 1D) again.

After the first method, Naor and Shamir (1997) improved their technique further to balance the contrast of the output image by diving the image into three semi groups (Red, Yellow and Transparent) instead of two (Black and White). In the meantime, Ateniese et al. (1996) proposed a method which showed n shares can be created from an image and only k or more than k shares can

Figure 1. Application of visual cryptography



be used to retrieve the image, but secret can't be revealed using less than k shares. In this paper the fundamental concept of visual cryptography has been used to generate the image share of the cover image in order to increase the embedding capacity of the proposed method.

2.2. Discrete Cosine Transform (DCT)

DCT is used to transform an image from spatial to frequency domain. As it has been explained by Li, Wang and Dong (2017), an image is composed of many pixel values and any change made directly in those pixel values can be immediately detected. Therefore, it is essential to transform them into their frequency domain. On doing so, it can be observed that on a set of 8x8 DCT block, cell (1,1) is most important. As it has been discussed by Gupta Banik and Bandyopadhyay (2015), this cell is known as the DC coefficient which holds the average value for the whole block and the other elements are known as the AC components which holds minor details of individual position. Thus, any change made in DC coefficient is easily visible as it effects the whole block. However, importance of all other cells varies. Based on this concept, a DCT block can be divided into three parts: High band frequency, Mid band frequency and Low band frequency. Any alteration made in mid band region are less likely to affect the image quality and therefore mid band cells are ideal to hide a secret. Figure 2 demonstrates the different bands in DCT.

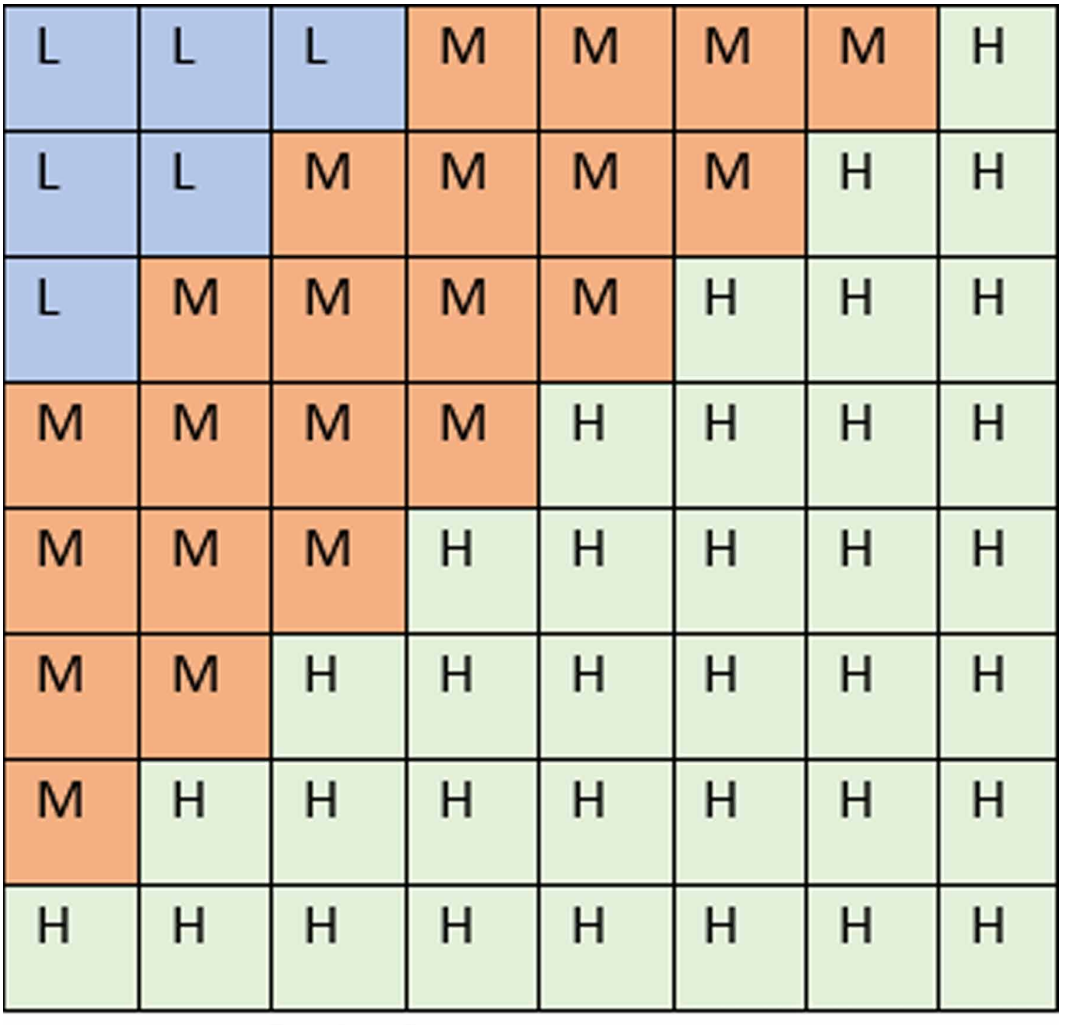
According to Tsai et al. (2017), an image in a spatial domain is represented as F(x,y) where x, y are constraints in spatial domain. Whereas in frequency domain it is represented as F(u,v) where u, v are constraints in frequency domain. Thus,

$$F(x,y) \xrightarrow{DCT} F(u,v) \tag{1}$$

Now, mathematically F(u,v) is given as,

$$F(u,v) = C * F(x,y) * C^{T} \tag{2}$$

Figure 2. DCT Bands (L for Low, M for Mid and H for High)



Where C^T is the transpose of *C* which is Discrete Cosine Transformation matrix which is given by,

$$C(m,n) = \sqrt{\frac{1}{N}} \text{ where u = 0 and } 0 \leq v \leq \text{N-1} \tag{3}$$

$$= \sqrt{\frac{2}{N}} * \cos\left\{\frac{\left(2v+1\right)\prod u}{2N}\right\} \text{ where } 1 \leq u \leq \text{N-1 and } 0 \leq v \leq \text{N-1} \tag{4}$$

2.3. Discrete Wavelength Transform (DWT)

DWT is used to split an image into high and low frequency components which helps to locate potential positions to hide a secret. According to Baby et al. (2015), this is mainly achieved through scaling the core wavelet by using high and low pass filters. DWT is applied on a wavelet which can be defined as a function of time and frequency. As described by Yadav and Dixit (2017), DWT having advantage over Fourier transform, which is applicable only to the frequency component whereas DWT can be applied to both time and frequency. DWT is based on Heisenberg's uncertainty principle, which states that one can have either high frequency resolution and poor time resolution or poor frequency resolution and good time resolution.

DWT provides a high frequency resolution for components with low frequency i.e. it gives the average intensity values of the image. On the other hand, DWT gives high temporal resolution for high frequency components i.e. for the edges.

Figure 3 shows the working principle of DWT which initially applies low pass filter on the original image to give the horizontal approximation and applies high pass filter on the original image to give the horizontal details. Subhendar and Mankar (2016) further narrated that by applying low pass filter on the horizontal approximated component, the final result is the average approximate value of the image represented as LL band and on applying high pass filter, the result obtained is the vertical detail component (LH band). In the same manner Al-Korbi et al. (2015) clarified when low pass filter is applied on the horizontal detail component, horizontal details are found (HL band) and on applying high pass filter, diagonal details is obtained as output (HH band). Thus, while applying DWT on an image, it transformed into 4 components (LL, LH, HL, HH). Further each of these band can be used as an image hence DWT can be applied on them individually thus giving multilevel DWT.

Figure 4 shows the basic concept of multilevel DWT and Figure 5 demonstrates the output of DWT on an image, where Figure 5A illustrates the original image. It is clear by the figures that the HH band shown in 5B holds the detailed values.

Figure 3. Working Principle of DWT

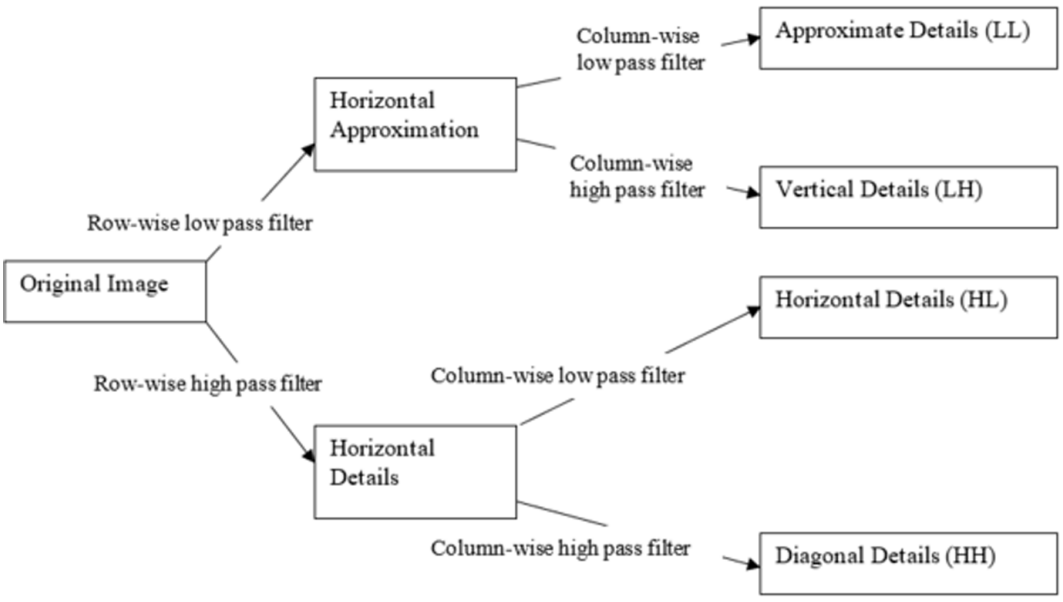


Figure 4. Multilevel DWT

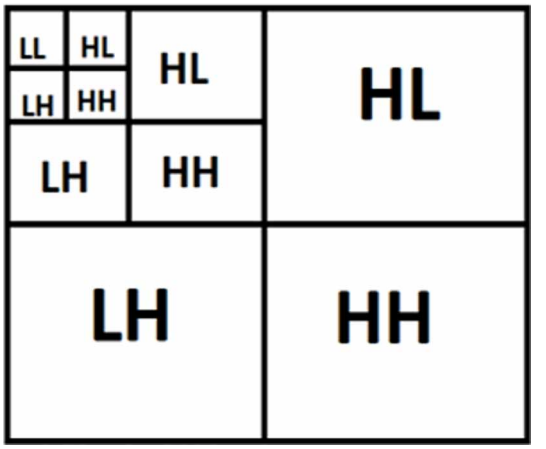
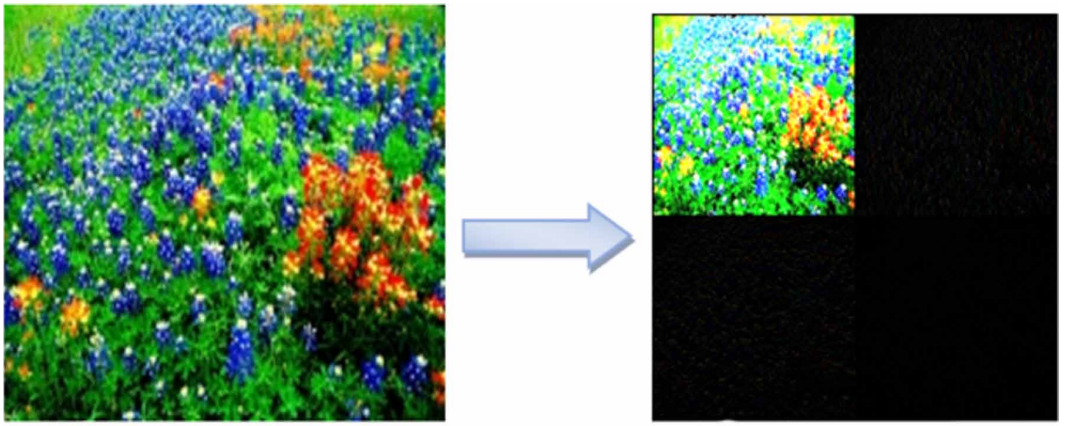


Figure 5. A) Original image before DWT; B) Image after applying DWT



2.4. Pseudo Random Sequence

Pseudo Random Number sequence is a sequence of numbers generated randomly. According to Najih et al. (2017), PN sequence is mainly used for encryption and embedding techniques because it increases efficiency, security and is robust. The most common way to generate a PN sequence is logistic mapping which is a key based generation, i.e. the values are generated based on a particular key. As described by Swami and Sarma (2014), one can define a 1-D logistic map as

$$y(n+1) = \lambda y(n)(1 - y(n)) \tag{5}$$

where, y(o) is the initial value, λ is a positive value such that $3.57 < \lambda < 4$ and n is the no. of iteration

It can be seen from the equation above, the $(n+1)^{th}$ bit depends on the nth bit. Thus, nth bit is used as a key here.

2.5. Correlation Coefficient

The term correlation originated from two words: 'Co' meaning "together" and 'relation' i.e. the statistical study of relation of two variables. It is the study of the linear or non-linear relation between two distinct continuous variables. Its value ranges in between -1 and +1. However, it is never possible to find an ideal similarity between two different variables, therefore the practical range is between -0.999 and +0.999. According to Zou, Tuncali and Silverman (2003), depending upon the type of distribution of the variables, one may use a linear correlation calculated by Pearson's correlation or a non-linear correlation by using rank correlation or Spearman correlation method.

Pearson's Correlation Coefficient is generally referred to as the correlation coefficient and is denoted by r. This method is used to find the linear relation between two variables. As described by Ranter (2009), for two variables X,Y, correlation coefficient r is calculated as

$$r = \frac{\left[X_i - Mean(X)\right]\left[Y_i - Mean(Y)\right]}{\sigma_x \sigma_y} \tag{6}$$

Where X_i and Y_i are the instantaneous values of X and Y; And σx, σy are the standard deviation of X and Y respectively.

Figure 6A shows perfect negative correlation i.e. with the increase of one variable, the other variable decreases linearly. Figure 6B shows perfect positive correlation i.e. with increase of one the other variable linearly increases. Figure 6C shows uncorrelated data where no relation can be formed and Figure 6D shows strong positive correlation.

3. PROPOSED METHOD

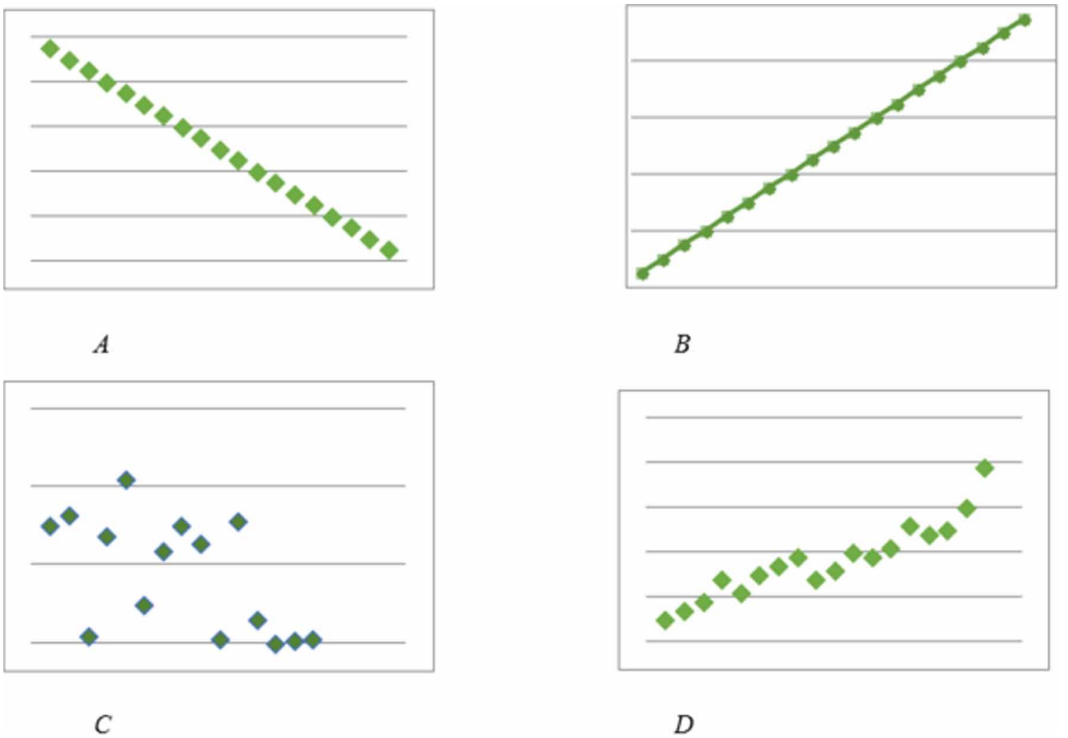
The purpose of this paper is to establish a novel, blind and robust image steganography algorithm which can embed multiple binary images in a single image. The cover taken is an RGB color image which has been split into three color planes (Red, Green and Blue) followed by each of this color planes has been further divided into two image shares by applying fundamental concepts of Visual Cryptography to enhance the embedding capacity. On top of these images, DWT is applied which helps to locate suitable band to hide a secret. Lastly DCT is applied on the selected band to enhance the security. The modified region is transformed back to the spatial domain and the components are integrated together to generate the Stego image. Similarly, at the receiver's end, fundamental concept of Visual Cryptography has been applied on the color planes of the Stego to retrieve the image shares followed by DWT and DCT and then by using correlation coefficients, the embedded secret is retrieved.

3.1. Embedding Procedure

3.1.1. Inputs and Outputs

In the method proposed, the Cover is RGB image and the secrets are binary images. An RGB image is a fusion of three grayscale images which has pixel values varying in between 0 and 255.The 3 grayscale components of RGB image represents its 3-color plane Red, Green and Blue. These three images are combined together to give a color 3D image of dimension m*n*3 where m*n is the size of each plane. In the method proposed, the cover is broken into these components and the rest of the process is applied on individual color plane which are grayscale images. On the other hand a binary image has only two-pixel values 0 and 1. 0-pixel value gives black color and 1 gives white so a binary image is simply a black and white image. Figure 7 shows the three different color planes of an RGB image.

Figure 6. A) Perfect Negatively correlated, r=-1; B) Perfect Positively correlated, r=+1; C) Uncorrelated, r=0; D) Strongly Positively Correlated=0.85



3.1.2. Applying Visual Cryptography

As outlined in section 2.1, Visual Cryptography splits an image into a number of shares which acts as separate images of same dimension as the original image and can be put back together to retrieve the original image. Here each plane is broken down in two image shares. These images contain partial values of the original image. If it is assumed that to embed a secret of p × q an image plane of m × n is required, then on applying visual cryptography on that image plane, two separate images of dimension m × n are formed so one can now embed one secret image of p × q in each of those two image shares. On doing so the embedding capacity for each plane doubles itself. In this paper, a plane is taken, and alternate column of data are saved in two separate images followed by a column of 0's to get the image shares and while retrieving, alternate column of data is taken from each plane and are saved as a new image which is the modified plane.

Algorithm to generated image shares

Step 1: Start

Step 2: Input IM as original plane.

Step 3: Create two blank matrixes A and B

Step 4: For all odd values of J and any value of I, where I is the row number and J is the column number, apply below:

- *A[I][J]=IM[I][J]*
- *B[I][J]=0*

Step 5: For all even values of J and any value of I, apply below:

- *B[I][J]=IM[I][J]*
- *A[I][J]=0*

Step 6: A and B are the images formed by applying the concepts of Visual Cryptography

Figure 7. Distribution of an RGB image into red, green and blue color planes

Step 7: End

On individual color planes, the aforesaid algorithm is applied to attain separate image images, as shown in the Figure 8 below. On doing so two separate secrets can be embedded on the two segments thus increasing the capacity.

Algorithm to build modified image from image shares

Step 1: Start
Step 2: Input A and B, the modified images
Step 3: Create IM matrix having same dimension of size of A and B.
Step 4: For all odd values of J and any value of I where I is the row number and J is column number, IM[I][J] = A[I][J]
Step 5: For all even values of J and any value of I, IM[I][J] = B[I][J]
Step 6: IM is the retrieved image.
Step 7: End

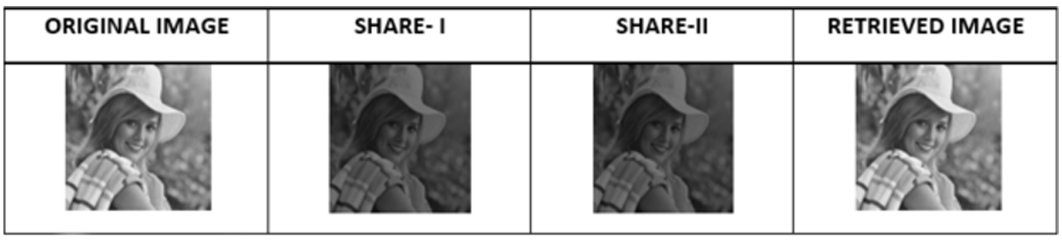
3.1.3. Selecting Ideal Position to Hide A Secret

Now on individual image shares, DWT is applied. As discussed in section 2.3 DWT divides an image into a number of bands. HH band carries most information. Therefore, changes made in this band are likely to be visible and so it is avoided for secret hiding. The other bands contain minor details and little modifications made on those are not visible. Thus, in this method DWT is used to select suitable locations to hide a secret. Here LL band is selected to hide a secret. DWT affects the size of an image. Once one-level DWT is applied on a m × n image, the output image dimension becomes m/2 × n/2.

Algorithm

Step 1: Start
Step 2: Input B as a color plane
Step 3: Apply DWT
Step 4: Save all 4 band in separate matrixes
Step 5: Select LL band to hide secret

Figure 8. Image Shares Creation and Retrieval by applying concepts of Visual Cryptography



Step 6: End

3.1.4. Obtaining Mid-Band Region

The selected LL band is further partitioned into blocks of size 8x8. On applying DCT, on each of these blocks, one finally gets access to (m/2 × n/2)/(8x8) mid band regions. For example, for a cover of size 1024 × 1024, when DWT is applied the selected band formed is of the size 512 × 512. On this when DCT is applied, a total of (1024/2 × 1024/2)/(8 × 8) = 64 × 64 mid-band regions are formed. As stated in section 2.2, DCT converts spatial domain into frequency domain thereby increasing the security of the whole process. It has been already established that secrets are embedded in the mid-band region only. In the method proposed, one-pixel value of the secret image is embedded in each of these mid-band regions. Thus, the number of mid band region formed is the maximum number of pixels of the secret image. So, for a cover of 1024 × 1024, the secret can be at max of size 64 × 64.

Algorithm to Obtain Mid-Band Region

Step 1: Start
Step 2: Input B as selected band
Step 3: Create blocks of 8x8 in B
Step 4: Apply DCT on individual Block.
Step 5: End

3.1.5. Generating PN-Sequence

In the meantime, two N-bit PN sequence are generated which along with a constant knows as the alpha factor is used to modify the mid-band region. The PN sequence in the method has been generated by a key based generator method similar to the one explained in section 2.4. The number of bits manipulated in each mid-band is denoted by N. Depending on this, the PN sequences are generated each of which is N-bit. Thus, there exists N separate PN sequence bits for N coefficients.

3.1.6. Modifying the pixel values

For each pixel value of the secret, there exists a specific mid-band. For example, for secret bit (1,1), the mid-band region corresponding to block (1,1) is modified. Similarly for secret bit (p,q), the mid-band region corresponding to block (p,q) is modified. The secret used is a binary one, hence there exist only two possibilities for the pixel values - 1 and 0. For pixel value 1, PN sequence 1 (PN1) is used and in the same manner for pixel value 0, PN sequence 2(PN2) is used.

Now bit wise scanning of the binary image is to be done. For bit value 1, all the selected coefficients of the corresponding mid-band region are modified using an alpha factor and the corresponding bit of PN1. The product of PN1 and alpha factor(af) is added to the coefficient thus causing the modification. Similarly, for a bit value 0, the coefficients are modified by adding to it the product of alpha factor and the corresponding PN2 bit. In both the case, there exists only two product value af* 0 and af*1. The changes made by the product af*1 persists but on the other hand the product af*0 which is 0 does not modify the coefficients at all hence secret can't be detected using these coefficients. Hence multiple coefficients are needed to be modified as effectively not all will be modified. Furthermore, if only 1 was added to the coefficients directly, the effective change after inverse DCT and inverse DWT would have been undetected. Hence the modification was needed to be amplified and to do this alpha factor was introduced to amplify the change by a value that would persist. This process is implemented for all the bits of the secret.

Algorithm to Modify Each Mid Band Region

Step 1: Start
Step 2: Input D as each block
Step 3: Initialize af
Step 4: Select appropriate positions to hide image from Mid-band region
Step 5: Scan B from the secret image as the corresponding bit for the Mid-band

Step 6: For each the positions denoted by P(x,y) and pos representing the bit number of PN sequences corresponding to P(x,y),

If B==1

- $P(x,y)=P(x,y)+af*PN1(pos)$

Else

- $P(x,y)=P(x,y)+af*PN2(pos)$

Step 7: End

3.1.7. Generating Stego Image

The modified blocks are again represented as a DCT band in frequency domain so, inverse DCT is applied to transform the frequency values back to the spatial domain values. This modified band along with the other three bands (LH, HL, and HH bands) which were not hampered are fused together to get the modified image share. The process is repeated for another secret with the other image share. Thus, embedding two separate secrets into the two shares of the same image. Next the two shares are combined to attain the final modified image which is a modified color plane of the original RGB cover. The same process is repeated for the other two-color plane. Therefore, in all by the use of this method a total of six secrets can be embedded in a single cover, two for each color plane. Finally, all the planes are combined together to give the modified RGB cover which is known as the Stego.

Algorithm to Generate Modified Image Share

Step 1: Start
Step 2: Apply IDCT on each block
Step 3: Represent the block as a sub band
Step 4: Apply IDWT using the modified band and the other three non-modified bands
Step 5: Result of Step 4 is the modified image share.
Step 6: End

Algorithm for The Entire Embedding Process

Step 1: Start
Step 2: Input C as RGB cover and S as Binary secret
Step 3: Break down the RGB cover into its 3 color planes
Step 4: For each color planes execute Steps 5 and 6.
Step 5: Apply Visual Cryptography's Fundamental Concept on the image planes to generate two image shares for each plane
Step 6: For each segment execute Steps 7 to 11
Step 7: Apply algorithm to select appropriate position on the image share
Step 8: Apply algorithm to achieve mid-band region
Step 9: Generate PN sequence PN1 and PN2
Step 10: For each mid band region apply algorithm to modify each mid-band region
Step 11: Apply Generate Modified Image Share Algorithm
Step 12: Apply algorithm on the two images share to generate modified color plane.
Step 13: Combine all 3 modified color planes to get the STEGO.
Step 14: End

3.2. Extraction Procedure

3.2.1. Attaining Modified Positions of the Stego

One of the key features of the method is its retrieving procedure being a blind one that is only the Stego (modified cover) is required and not the original cover. Similar to the embedding process, the Stego is broken into its three-color planes at first. Then by the use of the same Visual Cryptography concept the modified image shares are created for each color plane. To get the same band where the modification has been applied, DWT is applied on each segment. After this the LL band is again split into the number of 8x8 blocks as the size of secret. Now as the modifications were made in frequency domain, DCT is applied on individual blocks to convert it into its frequency domain. At this stage

we again get the modified mid-band regions. For each mid-band region, we create a matrix with the modified coefficients as its elements.

In order to attain the same mid band positions where the modifications were made, the same algorithms are re-used which have already explained in the embedding.

3.2.2. Retrieving

Two PN sequences of same size as the numbers of elements in the matrix are generated. As the PN sequence is generated by a key based method, the sequences thus created are the same as used in embedding procedure. Now we compute the correlation coefficient 'r1' for the mid-band coefficient matrix formed and PN1 and again 'r2' for matrix with PN2. As mentioned in section 2.5, Correlation coefficient is used to compute relation between two entities. Now if the value of r1 is found to be more than r2 for any block, it can be concluded that the bit used during embedding for that particular block has to be 1 as only for bit 1 there exists a relation between PN1 and the coefficients which yields a higher correlation coefficient value r1. Similarly, if r1 is less than r2, it can be concluded that the bit used for that block is 0 as for 0-bit value relation exists between the coefficient and PN2 yielding higher value of r2. In this fashion all the bits used during embed are retrieved back from all the blocks and stored in matrix format giving the retrieved secret. This process is implemented for both image shares for each plane, thus successfully extracting six distinct secrets. The detailed algorithm used for the extraction process is shown below.

Algorithm to Retrieve Bit from Each Mid-Band Region

Step 1: Start
Step 2: Create a matrix M with all the modified positions of the block.
Step 3: Calculate r1 as the correlation coefficient between M and PN1.
Step 4: Calculate r2 as the correlation coefficient between M and PN2.
Step 5: If r1>r2
bit=1
Step 6: Else
bit=0
Step 7: End

Algorithm for The Entire Extraction Procedure

Step 1: Start
Step 2: Input S as STEGO
Step 3: Separate the 3 color planes
Step 4: For each color plane, execute Step 5 and 6
Step 5: Apply Visual Cryptography's concept to get the modified image shares.
Step 6: For each image share, execute Steps 7 to 13
Step 7: Apply the algorithm to select appropriate position to get the modified band.
Step 8: Apply algorithm to achieve mid-band region in that band
Step 9: Create an empty matrix B
Step 10: For each mid-band denoted by M(x,y) where x,y indicates the block number execute Steps 11 and 12
Step 11: Apply algorithm to Retrieve Bit from each mid-band region and store the value in B.
Step 12: Reshape B as the dimension of the secrets to be retrieved.
Step 13: B gives the retrieved image from each segment.
Step 14: End

4. DISCUSSION AND ANALYSIS OF RESULTS

4.1. Embedding Capacity

Assuming the dimension of the cover image used is m x n and the size of each secret be $p \times q$. So, size of each color plane is $m \times n$. On applying fundamental concepts of Visual Cryptography to

generate the two image shares, the size still remains same as the shares having same dimension as original. Now on each such share, a secret of size p × q is to be embedded. As there are three (Red, Green and Blue) color planes for each cover image and for each plane, there are two shares hence in total there are six image shares, each of which is used to embed secret image of size p × q. So in total, six separate secrets of size p × q can be embedded in an RGB cover image.

When applying DWT on an image share, the dimension has been reduced to half. On top of that, DCT has been applied on each 8 × 8 block, hence for an 1024 × 1024 square image, post DWT the size of each image share becomes 512 × 512. For applying DCT, this 512 × 512 image share has been broken into 64 blocks, each of which having size of 8 × 8. Now applying mid-band DCT technique, each of these 8 × 8 blocks can hold one bit of secret image. Hence using this proposed method, a cover image of 1024 × 1024 size can hold six different secret images, each of which having size of 64 × 64.

Hence Embedding Capacity for this method can be expressed as:

Embedding Capacity = (Total Size of Secret)/(Total Size of Cover)
= (6*64*64)/(1024*1024) = 0.0234 = 2.34%.

4.2. Quality Metrices

There are various well-known parameters to exhibit the quality of an image. The quality analysis metrics used in this paper are as follows:

4.2.1. PSNR

PSNR is the abbreviation for Peak Sound to Noise Ratio. In this method, the initial image is assumed to be standard. After that the modified image is compared with the original image in order to identify the dissimilarities which are considered here as noise because the deviation is unwanted. PSNR is the ratio of maximum possible value of a signal to the noise present in the signal and the ratio is measured in dB. PSNR is calculated using Mean Square Error (MSE) which is the measurement of average squared difference between the standard value and the value at hand.

MSE and PSNR are calculated as follows:

$$MSE = \frac{\sum_{m,n} \left[X(m,n) - Y(m,n) \right]^2}{m * n} \tag{7}$$

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \tag{8}$$

Where, X, Y are two images, m, n gives the pixel position and R is the maximum difference in input data. PSNR and noise are inversely proportional therefore as noise increases PSNR value decreases. The more is the value of the PSNR the better is the quality of the image.

4.2.2. SSIM

Similar to PSNR, SSIM or Structural Similarity Index needs two images with one as the reference or ideal. Unlike PSNR, this process does not deal with absolute errors but also with different masking such as luminance masking and contrast masking. SSIM deals more with the interdependencies between spatially close elements. Its value ranges in between 0 and 1. It is calculated as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{9}$$

Where μ_x, μ_y, σ_x, σ_y and σ_{xy} are the local mean, standard deviation and covariance of x and y respectively. SSIM must be close to 1 or else differences between the images may be visible.

4.2.3. Maximum Difference

Maximum difference (MD) is the highest deviation between the original image and the modified image and shows the maximum error. Maximum difference and quality of the image is inversely proportional that is, MD should be low for better quality of an image. This is calculated as:

$$MD = \text{Max}| A(i, j) - B(i, j) | \tag{10}$$

Where A and B are the images and i, j shows the position of all the pixels.

4.2.4. Structural Content

SC or Structural Content measures the similarity between the structure of two images by correlation. For better quality of image SC must be low. It is expressed as:

$$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} X(i,j)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N} \mathrm{Y}(i,j)^2} \tag{11}$$

where, X is the standard image and Y is the modified image both of size M x N.

In following 8 tables demonstrate the result for embedding and extraction of secret messages. Here 4 sets of result have been explained with the features like PSNR, SSIM, Maximum Difference and Structural Content. Table 1, Table 3, Table 5, and Table 7 are for reflecting embedding result by comparing original vs. stego image; Whereas Table 2, Table 4, Table 6, and Table 8 are illustrating extraction outcome by comparing original secret images against the extracted secret images.

5. ROBUSTNESS TESTS AGAINST STEGANALYSIS ATTACKS

Detection of secret's existence in a cover image leads to vanquish the main objective of Steganography i.e. imperceptibility. According to Bartel (2000), there are two types of steganalysis attacks available. One of them is passive attack whose main focus is to reveal the presence of secret, but enhanced methods of steganography are very robust towards this kind of attacks. On the other hand, the second kind of attacks are active attacks, which are easy to implement as their main object is only to destroy the secret hidden in the Stego. Therefore, if attacks like rotation, resize, crop, noise are applied into the cover image, there is a huge chance of data loss. Here the proposed method has been put to test against some of these kinds of active attacks to show its resistance and effectiveness against them.

5.1. Rotate Attack

In case of active attack of rotation, the Stego image is rotated to a particular angle. Therefore, the image has to rotate back the same angle to retrieve the secret and some data loss occurs during that process. Here the Stego was rotated 45° which has been shown by Figure 9. The extracted secret and their quality analysis have been described in Table 9 which proves the robustness of the proposed method against rotation.

Table 1. Quality analysis of image set 1 (embedding)

ORIGINAL IMAGE	SECRET IMAGES	STEGO IMAGE	PSNR	SSIM	MD	STRUCTURAL CONTENT
			37.8745	0.9801	9.5367	1.0005

Table 2. Quality analysis of image set 1 (extraction)

ORIGINAL SECRET						
RETRIVED SECRET						
PSNR	69.6304	69.3408	72.4935	73.4626	74.7120	75.8034
SSIM	0.9998	0.9998	0.9999	0.9999	0.9999	1
MD	1	1	1	1	1	1
STRUCTURAL CONTENT	1.0063	1.0082	1.0035	1.0000	1.0034	1.0040

5.2. Cropping Attack

The active attack of crop is severe in an image as it introduces random data loss. Here the stego image was of size 1024 × 1024 and the secrets were of size 64 × 64. The stego image has been cropped from (300, 300) to (450, 350) shown is Figure 10 but as the result shows in Table 10, the proposed method is robust to crop attack.

Table 3. Quality analysis of image set 2 (embedding)

ORIGINAL IMAGE	SECRET IMAGES	STEGO IMAGE	PSNR	SSIM	MD	STRUCTURAL CONTENT
	  		37.7501	0.9417	9.5367	1.0006

Table 4. Quality analysis of image set 2 (extraction)

ORIGINAL SECRET						
RETRIVED SECRET						
PSNR	INF	INF	INF	INF	INF	INF
SSIM	1	1	1	1	1	1
MD	0	0	0	0	0	0
STRUCTURAL CONTENT	1	1	1	1	1	1

5.3. Resizing Attack

To test the method's robustness against the attack of resize, the stego image of 1024 × 1024 has been resized to 1700 × 1700. Here Figure 11 shows the stego image after resize attack and Table 11 shows the quality analysis of the secrets after retrieval, which proves the method's effectiveness against resize attack.

Table 5. Quality analysis of image set 3 (embedding)

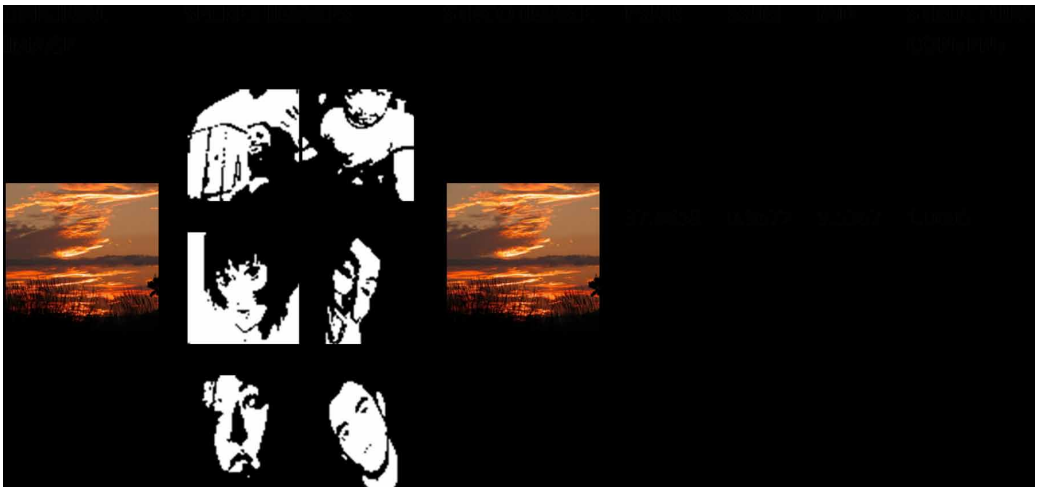


Table 6. Quality analysis of image set 3 (extraction)

ORIGINAL SECRET						
RETRIVED SECRET						
PSNR	70.4523	70.4523	70.6371	71.7017	69.3408	70.2750
SSIM	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
MD	1	1	1	1	1	1
STRUCTURAL CONTENT	1.0025	1.0076	0.9958	0.9829	1.0009	1.0097

5.4 Noise Addition

To put the proposed method to test against noise introduction, 20% Gaussian noise has been introduced to the stego image which is shown in Figure 12. Although it also introduces noise to the extracted secret images, the secrets are still recognizable, and quality is considerably good as depicted in Table 12.

Table 7. Quality analysis of image set 4 (embedding)

ORIGINAL IMAGE	SECRET IMAGES	STEGO IMAGE	PSNR	SSIM	MD	STRUCTURA CONTENT
			37.5731	0.9829	9.5367	1.0005

Table 8. Quality analysis of image set 4 (extraction)

ORIGINAL SECRET						
RETRIVED SECRET						
PSNR	71.2441	73.1150	75.8034	72.4935	75.8034	76.4729
SSIM	0.9999	0.9999	1.0000	0.9999	1.0000	1.0000
MD	1	1	1	1	1	1
STRUCTURAL CONTENT	1.0113	1.0086	1.0033	1.0072	1.0022	1.0015

5.5 Attack by Histogram Equalization

The histogram of an image is the graphical representation displaying number of pixels at each different intensity value present in that image. Histogram Equalizer is the method of contrast adjusting by removing the sharp edges from the histogram, so the output image has a uniform histogram where the

Figure 9. Stego image after 45° rotation

Table 9. Quality Analysis of secrets after Rotation of 45°

RETRIEVED IMAGE						
PSNR	57.4420	56.5680	57.6080	56.1791	57.7319	57.1448
SSIM	0.9887	0.9858	0.9880	0.9828	0.9883	0.9863

Figure 10. Stego after crop

image contains uniform distribution of intensity. Hence naturally huge amount of data loss occurs, and so the proposed method has been tested against histogram equalizer. Figure 13 shows the stego after histogram equalization applied and Table 13 shows the quality analysis of extracted secret images to prove the method's robustness against this attack.

6. COMPARISONS WITH EXISTING WORKS

Yuan (2014) has proposed an effective method of multi-cover adaptive steganography where an image is divided into n number of shares and the n shares are embedded into n cover images using secret sharing LSB method. Hence unlike the proposed method, this method's embedding capacity is inversely proportional to the number of shares because more shares will require more cover images to hide. The quality of the output images using proposed method are better compared to the aforesaid method of

Table 10. Quality analysis of secrets after crop

Yuan (2014). Another drawback of this method is that no steganalysis attacks have been performed to test its robustness. Therefore, the proposed method outcast the comparing method in all aspects.

Another existing method by Mostaghim and Boostani (2014) has used chaotic visual cryptography to enhance steganography. In this method, a chaotic map and the secret image is combined to create a share which is hidden in a cover image using DWT. However, in this article too, the method has not been tested against steganalysis attacks. Also, as per the PSNR values obtained in results, our proposed method produces better quality images which is more imperceptible. So even in this case, the proposed method proves it superiority against the comparing method.

The method depicted by Kumar and Kumar (2017), has implemented DWT similar to this proposed method and in order to validate the superiority of the proposed method, it has also been compared with the four other well-known existing techniques, which are as follows –

- DCT and DWT steganography technique by Kumar and Kumar (2010),
- Adaptive PVD based steganography technique by Swain (2016),
- Smart pixel adjustment-based steganography techniques by Yang and Wang (2015), and
- Overlapping block based PVD steganography techniques by Prasad and Pal (2017).

Here, comparison charts are provided in Table 14 and Table 15 to prove the excellence of this proposed method by comparing the highest and lowest values of PSNR achieved for stego and secret images respectively over all the above-mentioned methods.

The method introduced by Kumar and Kumar (2010), has used the combination of DCT with DWT and has tested the method against different steganalysis attacks like Gaussian Noise, Histogram Equalization, and Cropping Attack. A comparison of the PSNR values obtained in the extracted secret image is given in Table 16 to display the improvement achieved by the proposed method against those steganalysis attacks.

7. OPEN RESEARCH AREA

The proposed method can be applied further on Video Steganography and Watermarking without much alterations in the basic algorithm. Even though this method in the present form provides enhanced security to the classified images as the secrets are embedded after 3 layers of modification to the cover image, still the security of this proposed application can be further improvised by using different encryption techniques on the secret image, which can be considered as future scope of work.

8. CONCLUSION

This paper proposes an innovative image steganography method for RGB cover image which has been divided into two shares using a new technique similar to fundamental concepts of Visual Cryptography, to increase the number of image components because each of these components will

Figure 11. Stego after resizing

Table 11. Quality analysis of secrets after resize

RETRIEVED IMAGE						
PSNR	61.7017	61.3764	64.1684	63.6098	64.7120	65.3895
SSIM	0.9988	0.9986	0.9993	0.9993	0.9994	0.9996

Figure 12. Stego with 20% noise

Table 12. Quality Analysis of secrets after introducing 20% noise

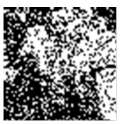
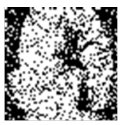
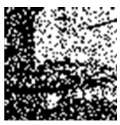
RETRIEVED **IMAGE**						
PSNR	54.6592	54.4955	55.2127	55.2453	55.1004	55.3615
SSIM	0.9913	0.9904	0.9927	0.9927	0.9927	0.9928

Figure 13. Stego after histogram equalization

Table 13. Quality analysis of secrets after equalizing histogram

RETRIEVED IMAGE						
PSNR	77.2674	76.4729	72.4935	72.2132	79.4832	79.4832
SSIM	1.0000	1.0000	0.9999	0.9999	1.0000	1.0000

Table 14. Comparison of the highest and lowest PSNR achieved by different methods for Stego image

Method Name	Highest PSNR of Stego Achieved	Lowest PSNR of Stego Achieved
Kumar and Kumar (2010)	34.6189	23.6012
Yang and Wang (2015)	34.7085	24.5689
Swain (2016)	34.7123	24.8137
Prasad and Pal (2017)	34.7819	25.1528
Kumar and Kumar (2017)	34.9175	25.9011
Proposed Method	37.8745	37.5731

Table 15. Comparison of the highest and lowest PSNR achieved by different methods for secret image

Method Name	Highest PSNR of Secret Achieved	Lowest PSNR of Secret Achieved
Kumar and Kumar (2010)	11.3466	10.2479
Yang and Wang (2015)	11.8634	10.5569
Swain (2016)	12.3823	10.5572
Prasad and Pal (2017)	12.7142	10.5599
Kumar and Kumar (2017)	13.7351	10.5619
Proposed Method	Infinite	69.3408

Table 16. Comparison of PSNR of secret images after different steganalysis attacks

Steganalysis Attack Name	Ref. Kumar and Kumar (2010)		Proposed Method	
	Highest PSNR achieved in extracted Secret	Lowest PSNR achieved in extracted Secret	Highest PSNR achieved in extracted Secret	Lowest PSNR achieved in extracted Secret
Gaussian Noise	19.50	15.52	55.3615	54.4955
Histogram Equalization	27.08	13.26	79.4832	72.2132
Cropping Attack	30.64	9.51	74.2544	68.0219

conceal a secret image. After that, DWT has been applied to obtain the ideal band for embedding the secret and then DCT has been used on those bands to convert it into frequency domain in order to increase the security. Subsequently, PN sequence has been applied to bit-wise embed each secret. The experimental results prove that the proposed method creates high quality stego images and can retrieve secret images without any data loss. The method has been thoroughly tested against several steganalysis attacks which demonstrate its robustness and imperceptibility. Lastly this proposed technique has been compared with five different existing methods and the comparison results clearly reflect that the proposed technique has outperformed all of those existing ones. The method has discussed in the context of RGB cover image which implies that it can be applied on grayscale cover image as well.

REFERENCES

Al-Korbi, H. A., Al-Ataby, A., Al-Taee, M. A., & Al-Nuaimy, W. (2015, November). High-capacity image steganography based on Haar DWT for hiding miscellaneous data. In 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT) (pp. 1-6). IEEE. doi:10.1109/AEECT.2015.7360552

Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual Cryptography for General Access Structures. *Information and Computation*, *129*(2), 86–106. doi:10.1006/inco.1996.0076

Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A Novel DWT Based Image Securing Method Using Steganography. *Procedia Computer Science*, *46*, 612–618. doi:10.1016/j.procs.2015.02.105

Banik, B. G., & Bandyopadhyay, S. K. (2015, November). Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in DCT. In 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) (pp. 400-405). IEEE. doi:10.1109/ICRCICN.2015.7434272

Bartel, J. (2000). *Steganalysis: An Overview, Security Essentials Bootcamp Style (Security 401)*. Global Information Assurance Certification Paper.

Dey, N., Roy, A. B., & Dey, S. (2011). A Novel Approach of Color Image Hiding using RGB Color planes and DWT. *International Journal of Computers and Applications*, *36*, 6.

Hemalatha, S., Dinesh Acharya, U., Renuka, A., & Priya, R. (2013). A Secure Color Image Steganography in Transform Domain. *International Journal on Cryptography and Information Security*, *3*(1), 17–24. doi:10.5121/ijcis.2013.3103

Kahn, D. (1996). The history of steganography. In R. Anderson (Ed.), *Information Hiding* (Vol. 1174, pp. 1–5). Springer. doi:10.1007/3-540-61996-8_27

Kumar, V., & Kumar, D. (2010). Digital Image Steganography Based on Combination of DCT and DWT. In V. V. Das & R. Vijaykumar (Eds.), *Information and Communication Technologies* (Vol. 101, pp. 596–601). Springer. doi:10.1007/978-3-642-15766-0_102

Kumar, V., & Kumar, D. (2017). Performance Evaluation of Modified Color Image Steganography Using Discrete Wavelet Transform. *Journal of Intelligent Systems*, *20170134*. doi:10.1515/jisys-2017-0134

Li, J., Wang, Y., & Dong, S. (2017, June). Video watermarking algorithm based DC coefficient. In 2017 2nd International Conference on Image, Vision and Computing (ICIVC) (pp. 454-458). IEEE. doi:10.1109/ICIVC.2017.7984597

Mostaghim, M., & Boostani, R. (2014, September). CVC: Chaotic visual cryptography to enhance steganography. In 2014 11th International ISC Conference on Information Security and Cryptology (pp. 44-48). IEEE. doi:10.1109/ISCISC.2014.6994020

Mukaka, M. M. (2012). A guide to appropriate use of correlation coefficient in medical research. *Malawi Medical Journal*, *24*(3), 69–71.

Najih, M. N. M., Rachmawanto, E. H., Sari, C. A., & Astuti, S. (2017, November). An improved secure image hiding technique using PN-sequence based on DCT-OTP. In 2017 1st International Conference on Informatics and Computational Sciences (ICICoS) (pp. 47-52). IEEE. doi:10.1109/ICICOS.2017.8276336

Naor, M., & Shamir, A. (1995). Visual cryptography. In A. De Santis (Ed.), *Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994*. Springer. doi:10.1007/BFb0053419

Naor, M., & Shamir, A. (1997). Visual cryptography II: Improving the contrast via the cover base. In M. Lomas (Ed.), *Security Protocols* (pp. 197–202). Springer. doi:10.1007/3-540-62494-5_18

Ogiela, M. R., & Koptyra, K. (2015). False and multi-secret steganography in digital image. *Soft Computing*, *19*(11), 3331–3339. doi:10.1007/s00500-015-1728-z

Prasad, S., & Pal, A. K. (2017). An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science*, *4*(4), 161066. doi:10.1098/rsos.161066 PMID:28484623

Ratner, B. (2009). The correlation coefficient: Its values range between +1/−1, or do they? Journal of Targeting. *Measurement and Analysis for Marketing*, *17*(2), 139–142. doi:10.1057/jt.2009.5

Rishi, R., Batra, S., & mr, R. (2011). Mode and Multiple Technique: A New Image Steganography Method for Capacity Enhancement of Message in Image. *International Journal of Computers and Applications*, *13*(1), 1–7. doi:10.5120/1770-2432

Sathisha, N., Babu, K. S., Raja, K. B., Venugopal, K. R., & Patnaik, L. M. (2011, July). Covariance based steganography using DCT. In International Conference on Advances in Computing and Communications (pp. 636-647). Springer. doi:10.1007/978-3-642-22714-1_66

Subhedar, M. S., & Mankar, V. H. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. *Computers & Electrical Engineering*, *54*, 406–422. doi:10.1016/j.compeleceng.2016.04.017

Swain, G. (2016). Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimedia Tools and Applications*, *75*(21), 13541–13556. doi:10.1007/s11042-015-2937-2

Swain, G., & Lenka, S. K. (2014). Classification of Image Steganography Techniques in Spatial Domain: A Study. *Engineering Technology*, *5*(03), 14.

Swami, D. S., & Sarma, K. K. (2014, February). A logistic map based PN sequence generator for direct-sequence spread-spectrum modulation system. In 2014 International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 780-784). IEEE. doi:10.1109/SPIN.2014.6777060

Tang, M., Hu, J., & Song, W. (2014). A high capacity image steganography using multi-layer embedding. *Optik*, *125*(15), 3972–3976. doi:10.1016/j.ijleo.2014.01.149

Tsai, S. E., Liu, K. C., & Yang, S. M. (2017). An Efficient Image Watermarking Method Based on Fast Discrete Cosine Transform Algorithm. *Mathematical Problems in Engineering*, 1–10. doi:10.1155/2017/3509258

Yadav, S. K., & Dixit, M. (2017, May). An improved image steganography based on 2-DWT-FFT-SVD on YCBCR color space. In 2017 International Conference on Trends in Electronics and Informatics (ICEI) (pp. 567-572). IEEE. doi:10.1109/ICOEI.2017.8300764

Yang, C.-Y., & Wang, W.-F. (2015). Block-Based Colour Image Steganography Using Smart Pixel-Adjustment. In H. Sun, C.-Y. Yang, C.-W. Lin, J.-S. Pan, V. Snasel, & A. Abraham (Eds.), *Genetic and Evolutionary Computing* (pp. 145–154). Cham: Springer International Publishing. doi:10.1007/978-3-319-12286-1_15

Yuan, H.-D. (2014). Secret sharing with multi-cover adaptive steganography. *Information Sciences*, *254*, 197–212. doi:10.1016/j.ins.2013.08.012

Zhou, Z., Arce, G. R., & Di Crescenzo, G. (2006). Halftone visual cryptography. *IEEE Transactions on Image Processing*, *15*(8), 2441–2453. doi:10.1109/TIP.2006.875249 PMID:16900697

Zhou, X., Gong, W., Fu, W., & Jin, L. (2016, June). An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS) (pp. 1-4). IEEE. doi:10.1109/ICIS.2016.7550955

Zou, K. H., Tuncali, K., & Silverman, S. G. (2003). Correlation and Simple Linear Regression. *Radiology*, *227*(3), 617–628. doi:10.1148/radiol.2273011499 PMID:12773666

Diptasree Debnath is currently studying for a Bachelor of Technology in Computer Science & Engineering at St. Thomas' College of Engineering & Technology. She has research interest in the field of steganography. She has coauthored 2 research articles in image steganography.

Emlon Ghosh is currently studying for a Bachelor of Technology in Computer Science & Engineering at St. Thomas' College of Engineering & Technology, Kolkata, India. He has research interest in network security domain and has coauthored 2 research articles.

Barnali Gupta Banik, B.Tech (Computer Science & Engineering), M.Tech (Software Engineering), Ph.D. (pursuing in Computer Science and Engineering from University of Calcutta, Kolkata, India), currently working as Assistant Professor of Computer Science & Engineering department at St. Thomas' College of Engineering & Technology, Kolkata. She has over 10 years of teaching experience and over 2 years of industrial experience working for MNCs in India and the UK. She has authored several research papers in the network security domain, including 10 Scopus indexed and 2 SCIE indexed articles.