IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Enhanced Security Mechanism Using Hybrid Approach of Watermarking

Deepakshi Mohal[1*], Sandeep Sharma[2]

[1,2]Dept. of Computer Engineering and Technology, Guru Nanak Dev University Amritsar, Punjab, India

[*]*Corresponding Author: deepakshimohal035@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i2.176189 | Available online at: www.ijcseonline.org

Accepted: 14/Feb/2019, Published: 28/Feb/2019

Abstract- In today's era the information is represented with the help of digital system. With the advancement of technology , now a days data is transmitted from source to destination with the help of images. Images are the source of data transmission. Data transmission through images is more secure as compared to the transmission through networked medium. In networked medium, the text can be easily sent and sometimes affected or may be harm by some third party or others. In this paper, we have provided two way security mechanism. Firstly, we have encrypted the text in the image and then in second phase we have placed one image on another image. Hence it is a two way security mechanism. Proposed system uses the hybridization of SVD-SLT techniques to secure the image and achieve better results in terms of accuracy. Two phases of digital image watermarking are used one of which is encryption and another is decryption. SVD (Singular Value Decomposition) will divide the image into parts and SLT (Slant Let Transformation) will merge two images overall resulting in watermarking. The result improvement is indicated through performance analysis with parameters PSNR, SNR, SSIM and through proposed mechanism 15% improvement is observed.

Keywords: *Truncated SVD, Modified SLT, Watermark, Encryption , Decryption, PSNR, SNR, SSIM.*

I. INTRODUCTION

Digital image processing plays critical role in defining security associated with the desired system. Image processing provides interactive way by which information can be represented. Interactive way is presented in the form of Graphical user interface. Security is critical in almost every field using technology. Several mechanism are proposed and several are under construction one way or the another , some modification to existing mechanism are required to tackle breach in security. To achieve the image security, watermarking and steganography mechanisms commonly followed. Image security mechanism plays vital role in this respect. These security mechanism includes:

1.1 Forgery detection

Forgery Detection is tampering the image to perform unauthorized alterations and manipulating it to cause damage. [1]The original photographic images can be manipulated to create the forged images, this process is known as digital image forgery. Forgery detection is the ability to detect forged and altered images. Image Forgery is the process of making illegitimate changes to an image information. Image forgery includes option of extra pixel or cutting some pixel force levels. Erasing some basic highlights is likewise objective related with image forgery. There are particular techniques which are utilized to forge a digital image, mulling over those strategy, [2] image forgery is partitioned into following classifications:

1.1.1 Copy Move forgery
1.1.2 Image Retouching
1.1.3 Segment Based Forgery
1.1.4 Image Splicing
1.1.5 Image resampling

1.1.1 Copy and Move Image Forgery

In this technique[3] , one part of image is changed and inserted into other part of the similar image. This technique` is used in manipulating the image.[4] Copy move forgery mechanism is also known as cloning. Some part of the image is cut in any size and pasted on some other region in this case. Critical information either is lost or replicated in his case as the copied part originated from the same image hence determining forgery becomes very difficult.

1.1.2 Image Retouching
This is generally less impactful phony component in which picture does not modify much. The picture highlights are lessened or improved for this situation. The complexity or shade of the picture is changed yet this kind of imperfections is hard to identify since picture adjustment isn't up to awesome degrees.

1.1.3 Segment Based Forgery
This is another seldom happening falsification component inside the picture. Picture is made out of extensive number of portions or squares. These pieces are sequenced. In this sort of phony, the sequenced squares are changed to mutilate the picture. expansive part of the picture is misshaped by the utilization of this fraud. Division components are required in requested to handle the issue.

1.1.4 Image Forgery Using Image Splicing
In Image splicing [3], [5] more than two images are joined together to create new one image and known as counterfeit picture. This is a standout amongst the most well-known sort of fabrication system. This component alongside the duplicate moves fashioned pictures are hard to distinguish since picture power levels does not contrast much from the first picture.

1.1.5 Image Resampling
[6] This is another basic technique for picture imitation. In this strategy some piece of the picture experiences transformation. Transformation incorporates interpretation, pivot, scaling and so on. The transformation utilized as a part of this case could be uniform or non-uniform. Uniform transformation does not modify the state of the picture. the non – uniform transformation then again adjust the state of the picture.

1.2 Image Steganography
The image steganography is the mechanism in which secret data is hidden behind the image. [7] In Steganography, the image is altered in such a manner that the sender and recipient can only detect or understand the message. In this process, we can hide text inside text, but we cannot hide text inside image .It replaces the bits with message bits so it is not that much secure like watermarking. In Steganography the existence of information inside the image or video is not visible or hidden from the user. To achieve the security in image, steganography as well as watermarking mechanisms commonly followed. The techniques for image security are described as under:

1.2.1 LSB Steganography
In LSB steganography[7], [8], the logo image is created by the replacing the least significant bits of the image. The contrast enhancement mechanism is implied in order to change the contrast of both the images so that merged images are clearly visible. Problem with this approach is however those attackers easily can determine the position of the logo and hence attack can easily takes place. In order to tackle the issue, MSB steganography is followed.

1.2.2 MSB Steganography
In MSB steganography[9], most significant bits are enriched with the logo image and hence merged image is obtained. The assumption is that MSB are less prone to attacks as compared to LSB bits. The mechanism of LSB steganography is performed in this case however MSBs are used in place of LSBs.

1.3 Image Encryption –Decryption
[10], [11]The encryption of image refers to transmission of image securely over the network so that any illegitimate or any unidentified user is not able to decrypt the image. The plain text is converted into cipher text by using encryption and any person is not able to read the message without using decryption mechanism. By using the reverse mechanism that is decryption the encrypted text is again converted into original plain text.
The techniques for image security are described as under:

1.3.1 Cipher Bits
This is another mechanism to ensure the safeguard of transmitted image over the career. The image meant to be transmitted over the medium however before transmission image is encoded and cipher image is obtained. The key that can be public or private is also generated. This key is transmitted along with the image itself. At the other end decryption mechanism is implied to resolve the problem into desired image formats. [12]

1.3.2 AES(Advanced encryption standard)

Advanced encryption standard can be used in order to provide encryption of images for security. [13]AES provide 128 bit encryption with 32 distinct segment formats. Keys are generated which are shared with sender and receiver. Keys are used to decode the image which is received at the destination end.

1.3.3 Image Authentication

This is the mechanism in which username and password is allocated to the image. In order to access the image username and password is required to be given. The wrong password ensures de-allocation of resources. [14]Image authentication is least secure since passwords can be easily guessed. In order to overcome this situation, image watermarking mechanism can be used.

1.4 Image Watermarking

Image watermarking involves multiple images that are merged together to achieve a common image that is transferred over a digital medium. [15], [16] Image watermarking is the process of placing information (text, image) into an image. Watermarking is a procedure through which one can cover up helpful data by the utilization of any digital media. Watermarking ensures that the data belongs to the owner and is read by the same user to whom it belongs. It is typically of two types:

a) Visible Watermarking
[17]Visible watermark comprises of either a visible message or the logo of an organization used to distinguish the proprietor. In visible watermarking, the watermark signal is visible in the image, video or content.
Example- Illustration Logo of the telecaster such as STAR PLUS, SONY and so forth is on the right top corner of the TV, it is visible to each client.

b) Invisible watermarking
In invisible watermarking, the watermark signal is not visible. The watermark is such that the watermark isn't visible to the client (Attacker). It is utilized to provide image validation and shield image from being duplicated. Invisible watermarking comprises of encoding process and translating process.

Basic principal of watermarking is given as under :

- Input the host image (primary image)

Figure 1: Primary Image

- Input the logo image(Secondary image)

Figure 2: Secondary Image

- Apply the mechanism of watermarking to merge the two images.


Figure 3 : Primary Image


Figure 4 : Secondary Image

- Output the watermarked image


Figure 5: Watermarked Image

Obtained the parameters such as PSNR, SNR and SSIM for performance measurement of techniques used.
In our research paper, in depth review of watermarking is done in order to enhance security in the transmission process. The other part of the paper is organized in the following manner: Section 2 provides earlier techniques used to enhance security of images along with comparative analysis of each of such technique. Section 3 provides the details of proposed systems. Section 4 gives the performance analysis and experimental results. Section 5 gives conclusion and future scope and last section gives the references.

II. EARLIER WORK

This section gives brief introduction of what exactly is done by the existing security techniques used within the digital systems. [18]Existing literature uses hybrid approach of DWT and SVD for enhancing watermarking security and uses fuzzy rules to identify malicious activity if any within the image while encoding and decoding of image.

2.1 DWT(Discrete Wavelet Transformation)

[19], [20]Wavelet Transform has transformed into a fundamental procedure for picture pressure. Wavelet based coding gives noteworthy change in picture quality at high pressure extents basically in light of better vitality of compaction property in wavelet transforms. Wavelets are capacities, which examine pictures and symbols, as demonstrated by scales or resolutions. The DWT addresses a picture in wavelet capacities by differentiating in scale and area is known as wavelets. It addresses the data with low pass and high pass coefficients. The experienced game plan data is of high pass and low pass channels and examined it. The outcome from low pass channel is harsh coefficient and the high pass is detail coefficient. This method is 1-D DWT but in research paper we are using 2-D DWT. In 2-D DWT two lines and segments are used. The yields are then down inspected by 2 toward each way as though there ought to be an event of one dimensional DWT. The four coefficients LL, HL, LH 2-D DWT comes out as outcome, and the data is experienced plan of both low pass and high pass channel and HH. Discrete Wavelet Transformation divides the image into 4 sub bands LL1, LH1, HL1 and HH1.These sub bands are less noisy and are simple in nature. Decomposition of sub-bands is highly independent.

$$W_{J,K}(T) = \frac{1}{\sqrt{2^J}} \quad W\left(\frac{T-K2^J}{2^J}\right) \qquad (1)$$

Equation 1 represents Wavelet Transformation. Here 'W' represent individual wavelet. 'T' is the time interval for which wavelet is obtained. 'J' is the scale parameter and 'K' is the shift parameter , both which are integers.

2.2 SVD(Singular valued decomposition)

SVD is a powerful technique which is employed in variety of applications.[21] Singular valued decomposition is used to reduce the complexity of operation. The SVD is a good way to extract geometric features from an image. SVD is used to perform linear algebraic transformation to decompose image into sub matrix. The entire image is decomposed into three parts and is represented in the form of matrix indicated with S, V and D. All the color dissimilarities are denoted with D and intensity mismatch is resolved with singular matrix s and v. SVD extract the matrix out of the available images by dividing it into parts. The overall operation is known as singular value decomposition.

$$M = SVD^T \quad (2)$$

Equation 3 can be represented using mode-k multiplication of matrix S, that is

$$M = Vx_1Sx_2D. \quad (3)$$

S, V, D are colored components. All the red color components are in variable S, similarly all the Green color components are stored in variable V and all Blue color components are stored in variable D. T denotes the transpose of a vector or matrix.

2.3 DCT(Discrete Cosine Transform)

In this transformation, outstanding estimation is consistently helpful in picture pressure. [22], [23]DCT changes over the pixels in a picture with different frequencies. This information is collected from spatial frequencies. It is the optimal method for estimation of the Karhunen_loeve transform and it gives the optimal pressure extent. The Discrete Cosine Transformation performs segregation on the different parts of the pictures. In quantization phase the parts of pressure truly occurs, then less key frequencies are discarded, from the original one. The remaining fundamental frequencies are utilized to recuperate picture during disintegration process. Therefore, revamped picture is contorted Format Based Approach.

$$Y(K) = \sqrt{\frac{2}{n}} \sum_{N=1}^{n} x(N) \cos\left(\frac{\pi}{4n}\ (2N-1)(2K-1)\right) \quad (4)$$

Equation 2 represents DCT transformation for discrete component K. 'N' is the total discrete components. 'x' is the distance of origin from the horizontal axes. 'n' is the number of simulations performed.

2.4 Shortcomings of the Existing Techniques:

DWT (Discrete Wavelet Transformation) divides the image into discrete wavelets. However ,when the integration of wavelets is performed problem at edges still remain, so discrete wavelet transformation does not perform that well in case images are distorted along the edges. DWT is less efficient and natural. It is computationally intensive. **SVD or Singular Values Decomposition** does not successfully operate on images which are complex in nature which means complex images remain unhandled in case of SVD. [18]DWT+SVD approach used in existing literature for watermarking image security when analysed for salt and pepper and poison noise, the results comes out be relatively on the higher side. Attack on watermarked image alters the image and it authentication is difficult to determine using DWT approach. **DCT (Discrete Cosine Transform)** algorithm is more suitable for the 2-D signal, but the images that comes as outcome will be in the RGB form. In our research work, the RGB images should be converted to gray scale images because the DCT algorithm can be performed on the 2-D array, but the RGB was already present in the 3-D array.

III. ENHANCED SECURITY MECHANISM USING HYBRID APPROACH OF WATERMARKING

3.1 Proposed System

The proposed system consist of DWT, SVD and SLT . In this, firstly we will resize the image to load it to attain the uniformity so that image fits in the axes. The resize operation will be applied to both the original image and the watermark image. After that the features of the components are extracted by the use of SVD and SLT. Once this operation is complete text encryption is performed with the image. The text encryption is performed at the most significant bit(MSB). After this the image will be stored within the buffer. The decryption side includes decryption of text from most significant position and inverse SVD-SLT is applied in order to obtain the original image from the watermarked image. Watermarking in existing literature is done by the use of discrete wavelet transformation. Advancement in terms of slant let transformation is giving better result in terms of parameters PSNR, SNR and SSIM. The proposed **methodology** will be given as under:

For Encryption

1. Obtain the input image.
2. Perform DWT and SVD for obtaining independent components from 2 different images.

3. Merge the images together using matrix operation.
4. Obtain the variance using SLT Transformation.
5. This is the process of encryption.

For Decryption

1. Obtain the input image.
2. Perform IDWT and SVD for obtaining independent components from 2 different images.
3. Demerge the images using matrix operation.
4. Obtain the variance using ISLT Transformation.
5. This is the process of decryption.

3.2 Methods used:

The proposed system uses truncated SVD in order to extract largest singular value where user specific parameter K specify the parameter magnitude. The advantage of using it is low dimensionality. The overall goal is to separate each component within the image for better identification of segments in case of watermarking.

SLT is modified through the application of selected data replication. With the help of SLT, reversible watermarking mechanism is formed and hence efficiently encrypted as well as decrypted.

We will use truncated SVD and modified SLT for text encoding and decoding. In text encoding we will encrypt the text in the image and in text decoding we will extract the hidden watermark from the image.

3.3 Parameters Considered :

3.3.1 PSNR

PSNR is Peak Signal to Noise Ratio. This ratio penalizes visibility of noise present in an image. It is a quality measurement between the compressed and original image. This parameter gives signal strength. Strength of signal is given in terms of noise present within the medium of transmission. Higher the noise least will be PSNR. Peak signal to noise ratio is high if noise occurs in the image is low. The higher the value of PSNR, the better reconstructed image can be achieved. This can be evaluated as

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \quad (5)$$

Here in the input image R is the maximum function data type and MSE is the Mean Square Error.

3.3.2 SNR

SNR is Signal to Noise Ratio (abbreviated **SNR** or ***S/N***). SNR can be defined as the ratio of the power of a signal and the power of background noise .In terms of image, how original image is affected by added noise. SNR is used to check the noise and error in the image. Signal to noise ratio is used to evaluate attack. Higher the value of SNR lesser is the chance of attack. The SNR will be evaluated as

$$SNR = \frac{P_{signal}}{P_{noise}} \quad (6)$$

3.3.3 SSIM

Structural Similarity Index is a method for measuring image quality. SSIM is used to measure the similarity in two images. SSIM is designed to improve peak signal-to-noise ratio (PSNR) and mean squared error (MSE). The SSIM index is a decimal value which lies between -1 and 1, and where the value 1 will occur in the case of two identical sets of data. The SSIM index is calculated for various windows of an image. The measure between two windows a and b of common size N*N is:

$$SSIM(a,b) = \frac{(2\mu_a\,\mu_b + c_1)\,(2\sigma_{ab} + c_2)}{(\mu_a^2 + \mu_b^2 + c_1)(\sigma_a^2 + \sigma_b^2 + c_2)} \quad (7)$$

Equation 9 represents the Structural Similarity Index. Here

μ_a represents the average of a

μ_b represents the average of b

σ_a^2 represents the variance of a

σ_b^2 represents the variance of b

σ_{ab} represents the co-variance of a and b

The flow of the proposed system is described in terms of the flowchart which is given below.

In first phase ,input the image i.e. primary image and logo image . After this resize both the images and then perform Feature extraction. Apply pre-processing mechanism for image enhancement to separate color components of the image. The separate the LSB & MSB bits to merge the image. Apply SVD and SLT for image watermarking and text encryption. To decrypt the image apply the inverse process and produce the result. Figure 7: represents the flow of the proposed system .

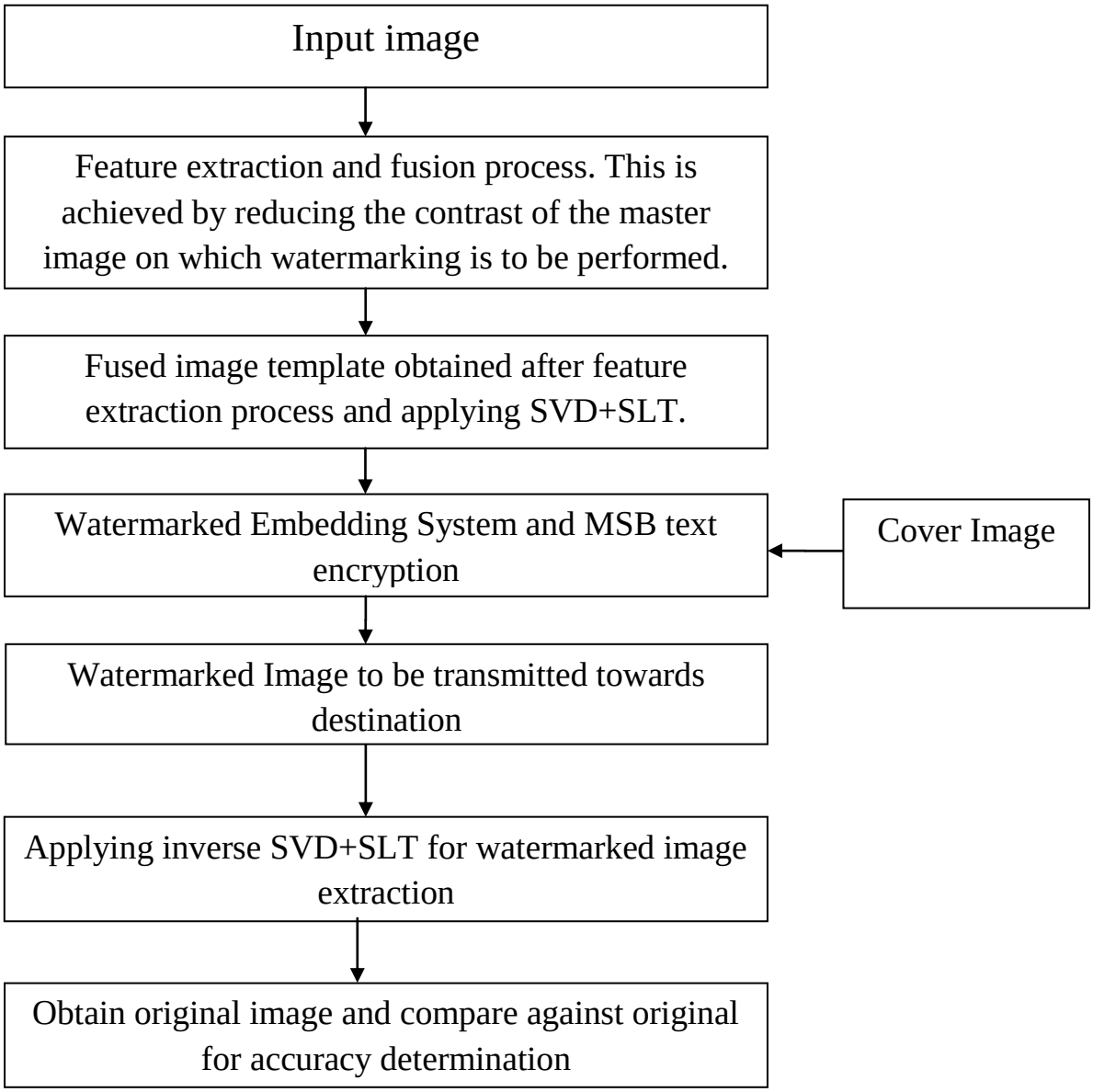


Figure 6: Flowchart of proposed methodology

Proposed Algorithm:

4.3.2 Proposed Algorithm:

The algorithm for the same is given as under

Step 1: Input image as host image(I) and convert it into Grayscale

I=imread(I);

I=rgb2gray (I)

Step2: Input logo image (I1) and convert it into Grayscale

I1=imread(I1)

I1=rgb2gray (I1)

Step 3: Apply DWT to transform the image into wavelets for complexity reduction

Apply Truncated SVD
Significance$_i$=I(:,1)
If(Significance$_i$>K)
I=I(:,1);
End of if

Significance$_i$=I1(:,1)
If(Significance$_i$>K)
I1=I1(:,1);
End of if

Step4: I3=cat(I,I1);// Concatenate the images together
Apply Modified SLT
Text=Input('Enter Text To Encrypt');
For i=Length(Text):1
I3(i+1)=I3(i)
End+
Merge the text
For i=1: length(Text)
I3(i)=Text(i)// Merging of text at most significant position
End

Step5: Decryption
Apply IDWT and ISLT for decoding
Produce the result in terms of PSNR, SNR and SSIM

IV. EXPERIMENTAL RESULTS

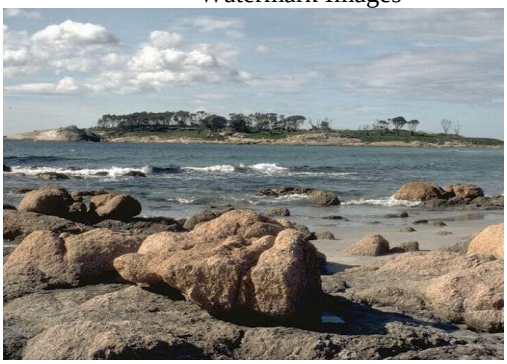
Digital watermarking is a productive strategy to ensure copyright and responsibility for data. It is the strategy for inserting digital data in any type of image and sound information, for example, picture, sound, video, and so forth .It is a technique for concealing one mystery information in another information. In earlier days watermarks were used as trademark or logo for demonstrating the responsibility for particular product. But in conventional techniques for digital picture watermarking, the surface of unique picture gets mutilated pretty much.

In proposed system noise is handled by component capable of introducing clarity within the image though filtering. In the wake of getting the clearness watermarking is forced. The picture information introduced to the reproduction is of .jpg and .png type. Results as far as PSNR, SNR and SSIM is acquired the coveted reproduction.
The dataset is derived from internet. The images are colored and are of different sizes. Hence resizing of images is needed.
Figure 7: given below shows the pictures that are used in this study work.

Primary Images

P1.jpg

Watermark Images



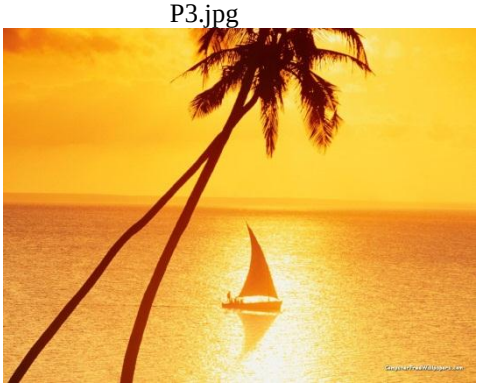
W1.jpg

P2.jpg

W2.jpg

P3.jpg

W3.jpg



P4.jpg

W4.jpg

P5.jpg

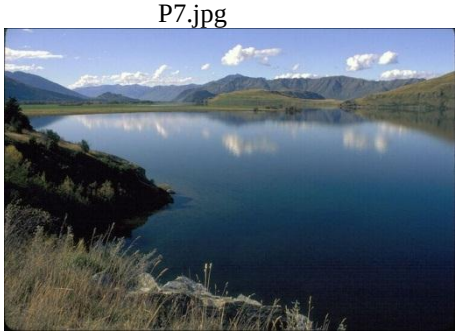
W5.jpg

P6.jpg

W6.jpg

P7.jpg

W7.jpg



P8.jpg

W8.jpg

P9.jpg

W9.jpg

P10.jpg

W10.jpg

Comparison of PSNR is given below:

Table 5.1: Comparison of Peak Signal to Noise Ratio

S.No.	Primary Image	Watermark Image	PSNR_Existing	PSNR_Proposed
1	P1.jpg	W1.jpg	22.5576	36.6888
2	P2.jpg	W2.jpg	22.6111	33.1681
3	P3.jpg	W3.jpg	22.5013	35.3159
4	P4.jpg	W4.jpg	22.2794	40.3048
5	P5.jpg	W5.jpg	22.4255	36.7805
6	P6.jpg	W6.jpg	22.68261	32.3328
7	P7.jpg	W7.jpg	22.3052	33.2506
8	P8.jpg	W8.jpg	22.6667	29.7685
9	P9.jpg	W9.jpg	22.4072	31.6142
10	P10.jpg	W10.jpg	22.1428	37.3398

Plots of PSNR with existing and proposed mechanism is given as under:

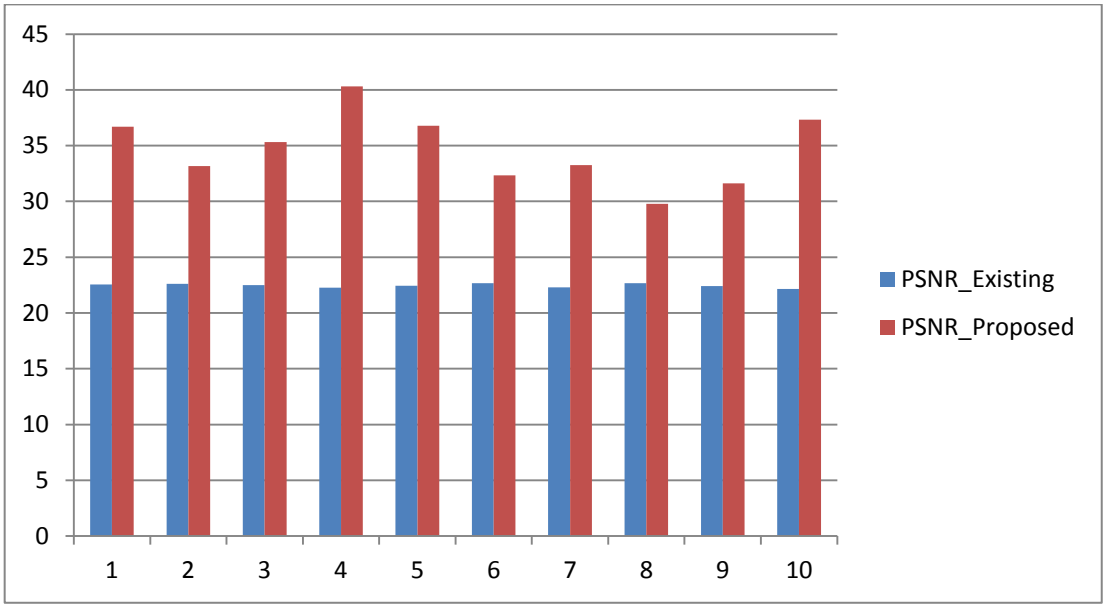


Figure 8 : Plots of PSNR with existing and proposed mechanism

Comparison of SNR is given below:

Table 5.2: Comparison of Signal to Noise Ratio

S.No.	Primary Image	Watermark Image	SNR_Existing	SNR_Proposed
1	P1.jpg	W1.jpg	15.7328	25.6005
2	P2.jpg	W2.jpg	17.9768	29.2594
3	P3.jpg	W3.jpg	15.2118	25.7507
4	P4.jpg	W4.jpg	16.6491	25.0543
5	P5.jpg	W5.jpg	16.4318	26.0473
6	P6.jpg	W6.jpg	16.1783	27.3394
7	P7.jpg	W7.jpg	14.404	24.2741
8	P8.jpg	W8.jpg	16.5336	28.4897
9	P9.jpg	W9.jpg	16.2743	26.6887
10	P10.jpg	W10.jpg	17.0169	25.8439

Plots of SNR with existing and proposed mechanism is given as under:

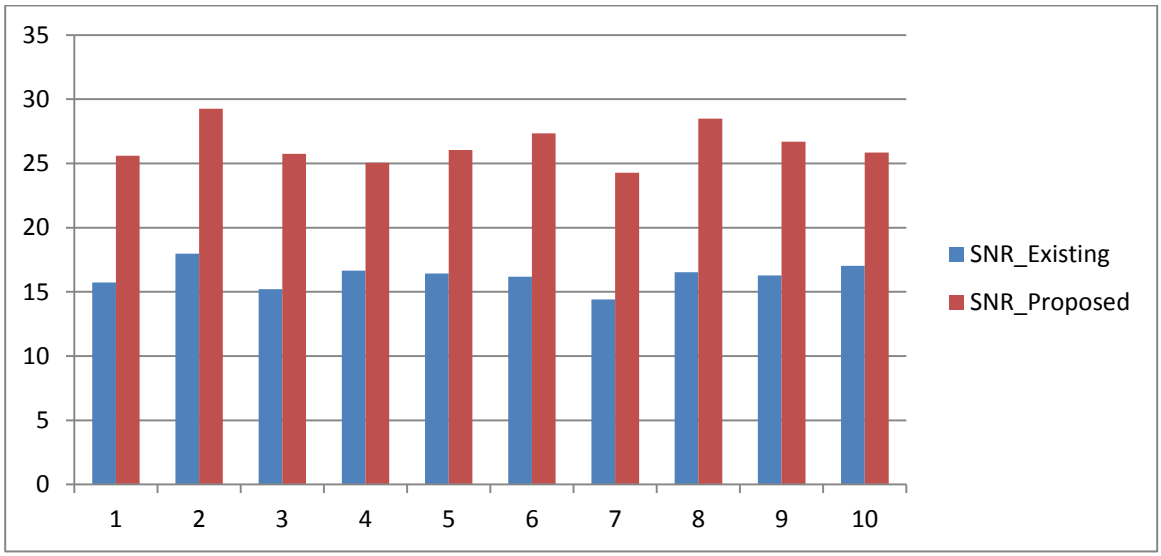


Figure 9: Plot of SNR with existing and proposed mechanism

Comparison of SSIM is given below:

Table 5.3: Comparison in terms of SSIM

S.No.	Primary Image	Watermark Image	SSIM_Existing	SSIM_Proposed
1	P1.jpg	W1.jpg	0.741621	0.858889
2	P2.jpg	W2.jpg	0.553969	0.87243
3	P3.jpg	W3.jpg	0.558425	0.86417
4	P4.jpg	W4.jpg	0.910044	0.844981
5	P5.jpg	W5.jpg	0.731969	0.858537
6	P6.jpg	W6.jpg	0.717465	0.875643
7	P7.jpg	W7.jpg	0.783607	0.872113
8	P8.jpg	W8.jpg	0.772909	0.885506
9	P9.jpg	W9.jpg	0.767874	0.878407
10	P10.jpg	W10.jpg	0.747099	0.856386

Plots of SSIM with existing and proposed mechanism are given as under:

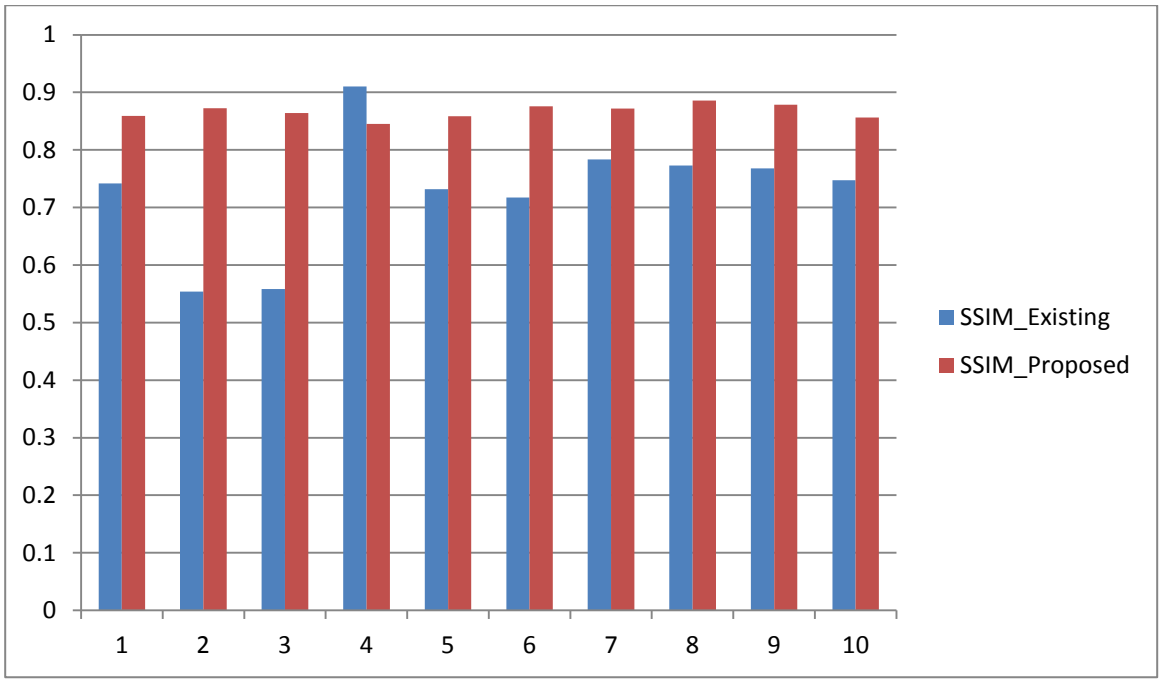


Figure 10: Plot of SSIM with existing and proposed mechanism

Result in terms of PSNR, SNR and SSIM of proposed system is better proving the worth of the study.

V. CONCLUSION AND FUTURE SCOPE

Information Transmission through computerized media is normal now days. As transmission through computerized media is extending chances of attacks are also occurs. During transmission information can be affected by disturbance, or by some unauthorized person which tries to get that information and modify the information. It can be secured by using advanced watermarks. If the sender needs to send some text or private picture to some individual, it will introduce the puzzle picture in another photo by using encryption technique and send it over the Internet. The recipient at the other side will get that image as input and concentrates that the concealed watermark from that picture with the assistance of the common key.

Security of information and picture will be of prime concern. Enhancing security is capable by the usage of number of frameworks consequently encryption and unscrambling instruments are basic. Encryption is typically performed on content information the scrambled content is regularly known as figure content. The software engineers may strike the encoded information since encryption frameworks are normally used. In order to redesign the security watermark shows up. The proposed approach enhancing the security by introducing clarity of picture encryption and deciphering through slant let changes. The SLT diminish the traverse of the image by breaking down it. By doing accordingly LSB and MSB bits of the image can undoubtedly be obliged. The results obtained through the proposed approach are better than the previous one. By the proposed mechanism, the result in terms of SNR, PSNR and SSIM is improved by 15%.

In future, real time dataset can be implied upon the proposed system. These real time datasets can be from real time environments like trees, plants etc. the accuracy and mean square error along with entropy showing degree of relationship between the pixel can be evaluated in future for proving worth of the study.

REFERENCES

[1] A. Doegar, “A Review Paper on Digital Image Forgery Detection Techniques,” *IEEE Access*, vol. 1, no. 3, pp. 1–5, 2015.
[2] S. Panda and M. Mishra, “Passive Techniques of Digital Image Forgery Detection : Developments and Challenges,” pp. 281–290, 2018.
[3] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, “Survey on Keypoint Based Copy-move Forgery Detection Methods on Image,” *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 206–212, 2016.
[4] A. Kuznetsov and V. Myasnikov, “A new copy-move forgery detection algorithm using image preprocessing procedure,” *Procedia Eng.*, vol. 201, pp. 436–444, 2017.

[5] H. Farid, "A survey of image forgery detection," *IEEE Access*, no. 4, pp. 1–22, 2009.
[6] A. V. Malviya and S. A. Ladhake, "Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram," *Procedia Comput. Sci.*, vol. 79, pp. 383–390, 2016.
[7] R. Mishra and P. Bhanodiya, "A review on steganography and cryptography," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 119–122, 2015.
[8] R. Bhardwaj and V. Sharma, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 832–838, 2016.
[9] C. G. Tappe and A. V Deorankar, "An Improved Image Steganography Technique based on LSB," *Int. Res. J. Eng. Technol.*, vol. 4, no. 4, pp. 2395–56, 2017.
[10] X. Li, "Digital Image Encryption and Decryption Algorithm W -- rn," *IEEE*, no. X, pp. 253–257, 2016.
[11] D. I. G. Amalarethinam, "Image Encryption and Decryption in Public Key Cryptography based on MR," *Comput. Commun. Technol.*, pp. 133–138, 2015.
[12] Y. V. S. Rao, S. S. B. Rao, and N. R. Rekha, "Secure image steganography based on randomized sequence of cipher bits," *Proc. - 2011 8th Int. Conf. Inf. Technol. New Gener. ITNG 2011*, pp. 332–335, 2010.
[13] D. M. Alghazzawi, S. H. Hasan, and M. S. Trigui, "Advanced Encryption Standard - Cryptanalysis research," *2014 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2014*, pp. 660–667, 2014.
[14] L. Rosales Roldan, M. Cedillo Hernandez, J. Chao, M. Nakano Miyatake, and H. Perez Meana, "Watermarking-based Color Image Authentication with Detection and Recovery Capability," *IEEE Lat. Am. Trans.*, vol. 14, no. 2, pp. 1050–1057, 2016.
[15] S. S. Gonge and A. Ghatol, "Intelligent Systems Technologies and Applications 2016," *IEEE*, vol. 530, pp. 85–97, 2016.
[16] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on Image Watermarking Algorithm based on DCT," vol. 10, pp. 1129–1135, 2011.
[17] U. H. Panchal and R. Srivastava, "A Comprehensive Survey on Digital Image Watermarking Techniques," *2015 Fifth Int. Conf. Commun. Syst. Netw. Technol.*, pp. 591–595, 2015.
[18] Anita and A. Parmar, "Image security using watermarking based on DWT-SVD and Fuzzy Logic," *2015 4th Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir. ICRITO 2015*, 2015.
[19] O. Jane, E. Elbaşi, and H. G. Ilk, "Hybrid non-blind watermarking based on DWT and SVD," *J. Appl. Res. Technol.*, vol. 12, no. 4, pp. 750–761, 2014.
[20] S. Bajracharya and R. Koju, "An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Image," *Int. J. Eng. Manuf.*, vol. 7, no. 1, pp. 49–59, 2017.
[21] S. A. H. Nair and P. Aruna, "Comparison of DCT, SVD and BFOA based multimodal biometric watermarking system s," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1161–1174, 2015.
[22] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on image watermarking algorithm based on DCT," *Procedia Environ. Sci.*, vol. 10, no. PART B, pp. 1129–1135, 2011.
[23] I. Conference and C. Engineering, "DWT DCT based New Image Watermarking Algorithm to Improve the Imperceptibility and Robustness," vol. 10, 2017.

