The Hybrid Approach for Image Watermarking using GLCM Algorithm

Rohit Singh, Simrandeep Singh, Nitin Sharma

ABSTRACT--- The image processing is the technology which is applied to process digital information in the form of pixels. The watermarking is the scheme which secure sensitivity image. The various schemes are proposed for the generation of watermark images. In the previous research work, the scheme of chaotic maps with Arnold transformation is used for the image encryption. The scheme of discrete wavelet transformation is applied for the image embedding. The bit selection for the image embedding is selected randomly which is inefficient approach. When the bits are selected randomly, the quality of watermark image degrades.In this research work, the gray level co-occurrence matrix algorithm is applied which select the embedding bit dynamically. The proposed scheme is implemented in MATLAB and compared with existing in terms of peak signal noise ratio, magnitude signal error and bit error rate.

Keywords:

Arnold transformation, Chaotic maps, Discrete Wavelet Transform (DWT), Gray-Level Co-occurrence Matrix (GLCM), Inverse Discrete Wavelet Transform (IDWT)

INTRODUCTION

Image processing is the technology which aims to improve the quality of features of raw images. It is possible to simplify the complex tasks with the help of image processing technology. Today, large numbers of applications are being setup on the basis of image processing technology [1]. There are certain complex tasks which are simplified using image processing. To improve the quality of features of an image, specific analysis tools are applied through this technology. The need of image processing is increasing every day due to the several benefits provided by it [2]. Different image processing applications have provided improvement in the visual appearance of images [3]. Further, the measurement of images can also be done through this technology. It is possible to perform both analog [4] and digital image processing in this technology. Imaging is known as the process through which acquisition of images is done [5]. It is also feasible to perform optical and analog image processing using this technique [6]. The images are generated from different fields such as computer graphics which can then be used for image processing. Image processing helps in manipulating [7] and enhancing the images. Computer vision is used to analyze the image [8]. An image consists of regions-of-interest which are present in the form of sub-images. An image consists of collection of objects that are considered as the base for a specific area. The appropriate region [9] is chosen in image processing by applying certain image processing operations. Thus, one part of an image is enhanced by using color rendition of an image [10]. The motion blur is suppressed using other part of the image. An image should be available in digitized form in image processing in the form of array. The given image is sampled on a discrete grid in the initial step of digitization process. For the quantization of each sample or pixel of an image, finite numbers of bits are used [11]. The digital images are processed using the computers. An analog signal is created by converting an image within this process. A digital image is then displayed by scanning this converted image. It is important to distribute the digital data since the information technology is improved [12]. The security level of data is enhanced when the development also increases. There are several attacks against which the multimedia data is to be protected. There are several techniques proposed for securing the networks against attacks [13]. Amongst them digital watermarking is the most commonly used technique. For securing the original data from illegal manipulation and distribution, a label, tag or information container is added within the multimedia data through watermarking technique. Visible or Invisible Watermarking are the two different types of watermarking approaches [14].A watermark embedder and a watermark detector are the two important components of digital watermarking system. It is possible to insert watermark on the cover signal using watermark embedder [15]. Further, the presence of watermark signal can be detected by the watermark detector. In the embedding and detecting watermarks process, an entity named the watermark key is utilized.

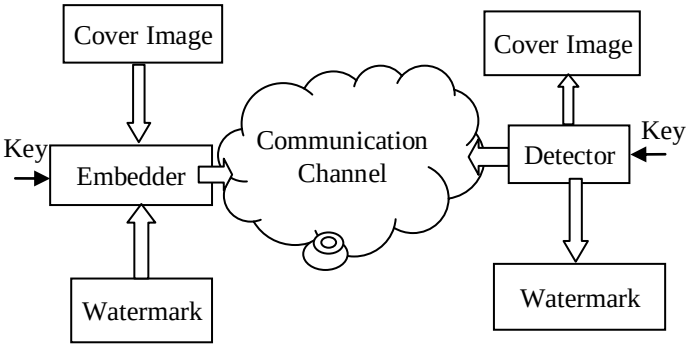

Fig-1: General Model of Digital Image Watermarking

PROBLEM FORMULATION AND CONTRIBUTION

The security is the major concern due to which various watermarking schemes are proposed in the previous times.

Revised Manuscript Received on May15, 2019.

Rohit Singh, Chandigarh University, Punjab, India. (E-mail: rohit.sambyal1740@gmail.com)

Simrandeep Singh, Chandigarh University, Punjab, India. (E-mail: simrandeepsingh.ece@cumail.in)

Nitin Sharma, Chandigarh University, Punjab, India. (E-mail: nitinsharma.ece@cumail.in)

The techniques which are proposed so far are not robust towards various security attacks such as contrast, salt & pepper and sharpen attack.The technique is required which should be robust towards various types of security attacks. The technique which is proposed so far for the watermarking has less quality of the watermarked images. Due to which efficiency of the watermarking scheme is reduced this needs to improve. The technique which is designed generate high quality watermark image.

This research work is related to increase the quality of the watermark image. When the quality of the watermark image is high then at the time of watermark extract, the quality of original image get retained. The embedding bit is selected dynamically in this research work, using gray level co-occurrence matrix. The gray level co occurrence matrix algorithm calculate textural features of the image and based on the textual features bit is selected for the embedding to generate watermark image.

In this paper, the introduction is presented in the first section. The introduction presents the introduction about the watermarking. In the second section literature review is written which highlight the previous research work. The research methodology is presented in the next section. In the research methodology section, the novel approach is presented in detail. The result and discussion is shows which describe comparative results of the proposed and existing techniques.

RELATED WORK

Abhilasha Singh, et.al (2018) proposed a novel sturdy zero-watermarking approach for medical images to deal with the confidentiality and safety concerns [16]. The proposed approach was based on Wavelet Transform-Singular Value Decomposition. The proposed approach protected the trustworthiness of the cover picture without causing any remains. The proposed approach did not alter the important data enclosed in the medical picture. Tele-ophthalmological images were used to evaluate the performance of proposed approach. The simulation outcomes depicted that the proposed approach was quite robust against several image processing intrusions. These outcomes also indicated the appropriateness of proposed approach for the secure sharing of medical pictures in the midst of distant medical professionals.

SubratoBharati, et.al (2018) stated that Discrete wavelet transform, Discrete cosine transform, bacterial foraging optimization (BFO) and particle swarm optimization approaches had been implemented [17]. The performance of these approaches was scrutinized for the watermarking of the medical picture. The comparative performance of the applied algorithms was computed in terms of PSNR (Peak signal to noise ratio) value, NCC (normalized cross correlation) and IF (image fidelity) parameters. It was identified that the Peak signal to noise ratio value and normalized cross correlation must be large for high-quality information enclosing.

Nasir N. Hurrah, et.al (2017) proposed a proficient watermarking approach on the basis of hybrid transform realm [18]. The proposed watermarking approach was blind, strong and safe. The approach was designed to deal with dual attacks. These attacks could be the combination of signal processing and geometric attacks. To achieve these objectives, a single watermark had been enclosed in all the three components (RGB) of the color image with the help of a novel interblock differentiating technique in discrete cosine transform (DCT) realm. The tested outcomes proved the robustness of proposed approach against all kind of signal processingattacks and geometric attacks. Furthermore, two instantaneous attacks on watermarked picture were executed for proving the sturdiness of proposed approach. The achieved outcomes for various attacks were provided on the basis of certain parameters such as Peak signal to noise ratio, normalized cross correlation, BER and BCE.

ImaneAssini, et.al (2017) suggested the multiple watermarking scheme[19]. The approach is the combination of three algorithms which are SVD, DWT and FWHT. The main benefit of this scheme is that the two images are embedded into the single image. The final image will be divided into third level of DWT. The similar procedures were applied on the primary watermark picture. Also, the second watermark image was divided till the initial level. This watermark picture was changed through singular value decomposition (SVD) scheme. The two watermarks were inserted in the singular values of the actual picture. The tested outcomes proved the supremacy of proposed approach in terms of improved cooperation invisibility, ability and sturdiness

HansaMehra, et.al (2017) defined a novel FDW procedure on the basis of discrete cosine transform with distinct dimension of actual and watermark pictures [20]. In this study, DCT transform technique was applied with the help of mid frequency segment. The method which is proposed is suggested in this work, generate watermark image which is secure and quality of the image is also good. The PSNR values were compared with the help of several test pictures. On the basis of PSNR values, it was concluded that Lena image had highest PSNR while Baboon image had least PSNR. Therefore, these two images had been utilized for detecting the effects of various noise attacks.The PSNR value was extremely fine after the consideration of additive noise. Thus, it was identified that the proposed approach was quite robust in opposition to the intended conspiracy and additive noise intrusion.

R. Surya PrakasaRao, et.al (2016) defied a watermarked scheme which is based on the genetic algorithm [21]. To generate the watermarking image, the three levelDWT method is used in this research work. When the watermark image is generated on that image SVD technique is applied to improve quality of the watermark image. The genetic algorithm is applied in the last for the calculating of scaling factor. In GA algorithm, PSNR and NCC parameters were utilized as fitness functions. These parameters were used for evaluating the sturdiness and insignificancy of watermarking method. Tested outcomes depicted that the proposed approach could survive against different kinds of image processing attacks robustly.

DhekraEssaidani, et.al (2016) proposed a novel strong, blind and undetectable watermarking scheme [22]. This scheme was based on an improved Delaunay triangulation approach. This approach was created with the help of features contents of the cover picture. MATLAB tool was used to perform computer simulations. These simulations were implemented on hundred pictures gathered through online. These images had been utilized for verifying the strength of the proposed watermarking approach. The novel Delaunay triangulation approach provided a significant strength to some contemporary and non-contemporary attacks on the basis of its structure. This strength permitted the building of a strong watermarking algorithm against a number of attacks.

Table 1: Table of Comparison

Author	Technique	Outcome
A. Singh [16]	The proposed approach was based on Wavelet transform-Singular Value Decomposition. The proposed approach protected the trustworthiness of the cover picture without causing any remains.	These outcomes also indicated the appropriateness of proposed approach for the secure sharing of medical pictures in the midst of distant medical professionals.
S. Bharati [17]	In the research work three methods are applied which are DWT, DCT, BFO and swam optimization.	The performance of the proposed algorithm is terms of PSNR, MSE and NCC which is normalized correlation
Nasir N. Hurrah[18]	The proposed watermarking approach was blind, strong and safe. The approach was designed to deal with dual attacks. These attacks could be the combination of signal processing and geometric attacks. To achieve these objectives, a single watermark had been enclosed in all the three components (RGB) of the color image with the help of a novel interblock differentiating technique in discrete cosine transform (DCT) realm.	The achieved outcomes for various attacks were provided on the basis of certain parameters such as Peak signal to noise ratio, normalized cross correlation, BER and BCE.
ImaneAssini [19]	In the proposed approach, two watermark images were embedded into a particular cover medical picture. The authentic medical picture was divided till the third level of discrete wavelet transform.	The two watermarks were inserted in the singular values of the actual picture. The tested outcomes proved the supremacy of proposed approach in terms of improved cooperation invisibility, ability and sturdiness
H.Mehra [20]	A novel frequency domain watermarking procedure on the basis of discrete cosine transforms with distinct dimension of actual and watermark pictures [20]. In this study, DCT transform technique was applied with the help of mid frequency segment. This was an averaging coefficient method used for extra secured watermarking algorithm of PSNR	The PSNR value was extremely fine after the consideration of additive noise. Thus, it was identified that the proposed approach was quite robust in opposition to the intended conspiracy and additive noise intrusion.
R. Surya Prakasa [21]	The proposed approach was based on Genetic Algorithm. In the proposed approach, watermark was embedded in third Level Discrete Wavelet Transform (DWT) of actual picture for its improvement	These parameters were used for evaluating the sturdiness and insignificancy of watermarking method. Tested outcomes depicted that the proposed approach could survive against different kinds of image processing attacks robustly.
DhekraEssaidani [22]	This scheme was based on an improved Delaunay triangulation approach. This approach was created with the help of features contents of the cover picture. MATLAB tool was used to perform computer simulations	This strength permitted the building of a strong watermarking algorithm against a number of attacks.

RESEARCH METHODOLOGY

a. Chaotic Maps

The chaos-based image encryption scheme has the two steps which are performed on the input image. In the process of image encryption, each pixel of the image is processed for the final stage of pixel permutation. The disordered behavior of the image is controlled by the 16 character key which is generated from the image. The chaotic encryption method has various phases, the pixel value of image get changes in the second phase. When the pixel values of the image get changes in the second phase it increase security of the image. When the security of the image get improved it directly increase security and also provide shield towards various type of security attacks

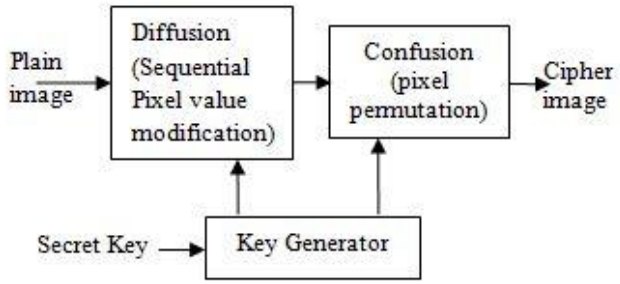

Fig. 2: Architecture of Chaos-based image encryption Method

The confusion stage is the important in which places of the pixels get shuffled without modifying pixel values. In the confusion stage image is not recognized easily which increase security.The shuffling of the pixels donot provide complete security to the image because, bit shuffle can be easily broken down. The key is generated which can modify the pixel values of the image. When the pixel values of the image get changes it directly improve image security. The chaotic encryption process is the complete diffusion process in which two stages are applied to increase image security. Every stage depends upon the other stage for the secure image generation.

b. Arnold Transform

The Arnold transform is an image scrambling technique that can be used to encrypt and decrypt image data. The transform is area preserving and invertible without loss of information. It is also known as cat map. The mapping can be done successively several times to completely obscure the image beyond recognition. Alice has the information about the number of times the transform is applied and can successfully recover the original image.

The Arnold transform of a two-dimensional image is defined as:

$$A^M : \begin{bmatrix} u_i \\ v_i \end{bmatrix} = mod\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x_i \\ y_i \end{bmatrix}, M\right), \quad \ldots(1)$$

In the above equation, $(x_i, y_i)$and $(u_i, v_i)$are pixel coordination before and after the Arnold transformation. The "mod" operation is applied when the division operation is applied on the image. The size of the image is calculated after which period p transformation is done. The Arnold transformation can scramble the image with the n number iterations.

c. DCT

The image is divided into parts of varying importance with the help of discrete cosine transform (DCT) depending on the visual quality of an image. Any signal or image that exists in the spatial domain is transformed into the frequency domain through DCT. The equation given below defines a general representation of 1D DCT:

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i).cos\left[\frac{\pi.\mu}{2.N}(2i+1)\right] f(i) \ldots(2)$$

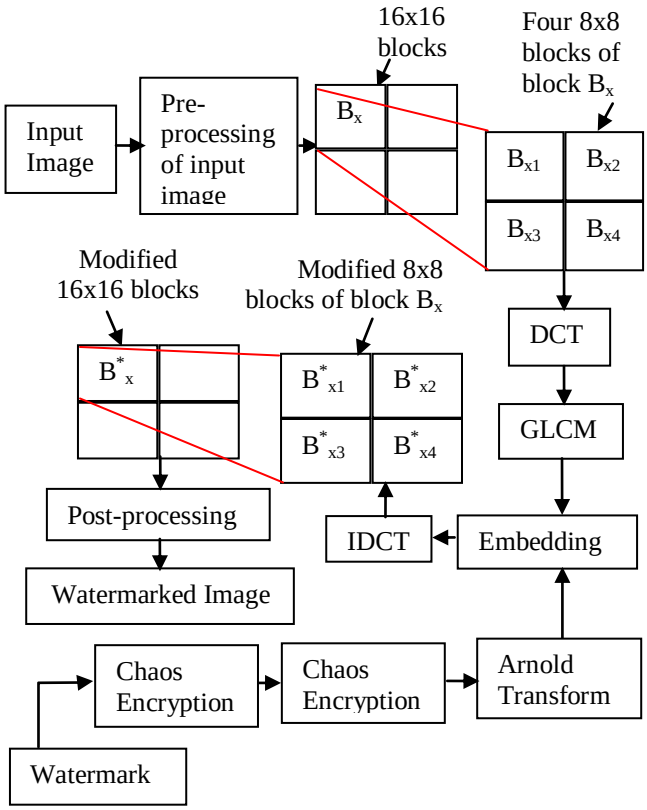

Fig 3: Block diagram of the proposed technique

d. Watermark Embedding

The four bits of encrypted watermark 'we' are embedded for a given 16×16 block such that each pair of DCT blocks includes one bit in them. On the basis of pre-embedding different that exists amongst two coefficients, 'D' is taken either to zone 2 or zone 5 such that bit '1' can be hidden. In case when 'D' lies in between zone 1 or 3, the coefficients $C_{xy}(i,j)$and $C_{xy+1}(k,1)$ are enhanced such that the difference that exists amongst them ranges to zone 2 which is the zone that is the closest to it. The two chosen coefficients are enhanced such that the differences can reach to zone 5 in case if the difference 'D' exists in zone 4. Therefore, the information about bit '1' can be carried by zone 2 or zone 5. There is degradation in the quality level of image due to the improvements made in the difference to the closest zone which is however very less in comparison to the other scenario in which the difference is enhancement to the zone that is the farthest. In similar manner, in case when the difference exists within zone 2, it is enhanced upon zone 1 such that bit '0' can be embedded. Also, the difference is enhanced up to zone 4 if it exist either in zone 3 or 5. A guard band of 2S is used to differentiate the difference zones for a specific bit. The robustness of proposed watermarking technique is decided by S which is known as the embedding strength. The extraction part highlights the extra robustness that is provided to proposed watermark through this guard. From within the range of 5 to 20, the value of S is chosen here. The value of S shows direct proportionality to the robustness of

system and inverse proportionality to imperceptivity. The IDCT for every enhanced DCT block is calculated once the embedding process is completed. Further, post-processing operations are performed after IDCT. A final watermarked image is generated when the post-processing operations are completed.

e. Gray-Level Co-Occurrence Matrix

The gray level co-occurrence matrix method can extract the textual features of the image which is of second order. The GLCM algorithm can provide the positions of the pixels which have same gray level. The GLCM algorithm can be applied on the image which has equal number of rows, columns and also gray levels. Two pixels that are separated by distance d and fall in the direction specified by angle (θ), one holding the intensity i and the other holding intensity j in a matrix have the relative frequency of $P(i,j|d,\theta)$. The MATLAB has the function which is named as graycomatrix which is used to create GLCM matrix. The GLCM matrix is further processed to calculate further second order textural features. The numbers of intensity values in grayscale image are reduced from 256 to eight when scaling is applied by default through graycomatrix. The size of GLCM is determined by the numbers of gray levels. The NumLevels and GrayLimits parameters of graycomatrix function are used for controlling the number of gray levels in GLCM and scaling the intensity values.

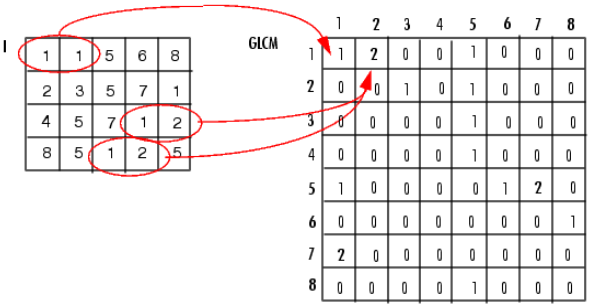

Fig.4: Working of gray level co-occurrence matrix

As illustrated in the figure 4, the pixel values of the image is shown. When the GLCM algorithm is applied on the input image it is will calculate the pixel intensities which are shown in the second matrix. The pixels of the image are processed vertically and horizontally to generate final results of the GLCM algorithm.

RESULT AND DISCUSSION

This research work is related to digital watermarking. In the existing technique, DWT is used for the watermarking generation. The Arnold transformation is applied to transform the image and generation of final watermark image. In the proposed scheme the GLCM algorithm is applied for textual feature analysis. The proposed methodology and existing schemes are implemented in MATLAB.

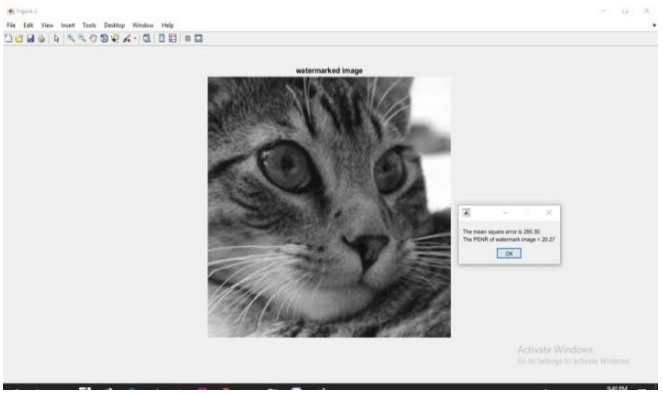

Fig 5: Watermarking image

As shown in figure 5, the GLCM based hybrid model is applied for the generation of watermark image. The DWT algorithm is applied for the image embedding. The watermark image is shown in this figure

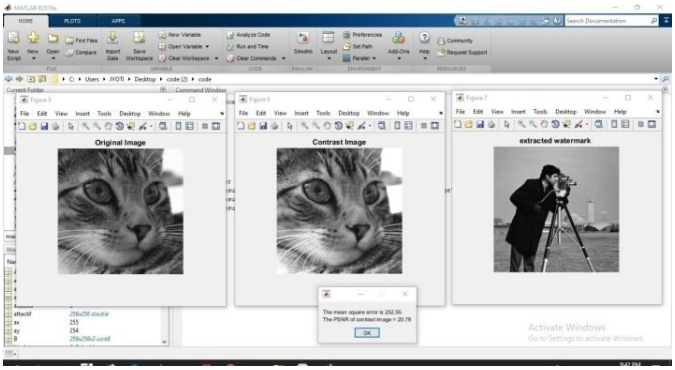

Fig 6: Inverse discrete wavelet transformation forExtraction

As shown in figure 6, the inverse DWT algorithm is applied which extract sensitive image from the watermark image

Table2: Peak to signal noise ratio comparison

Image Name	DWT Algorithm	GLCM Algorithm
Leena	20.33	24.40
Taj	20.46	24.55
Cat	20.27	24.33
Bear	20.25	24.30
Mona Lisa	21.61	25.93

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

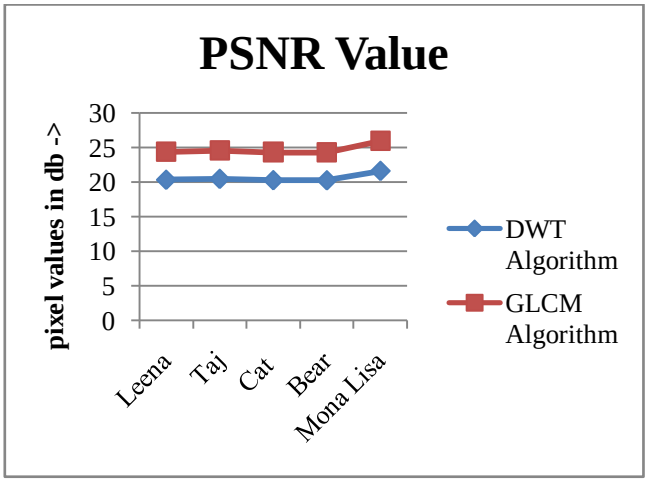

Fig 7: PSNR Comparison

As shown in figure 7, PSNR value of DWT and GLCM algorithm is compared for the performance analysis. The PSNR value of the GLCM algorithm is high as compared to DWT algorithm

Table 3: MSE Comparison

Image Name	DWT Algorithm	GLCM Algorithm
Leena	285.80	238.16
Taj	275.93	229.94
Cat	290.30	241.91
Bear	292.45	243.70
Mona Lisa	200.78	167.32

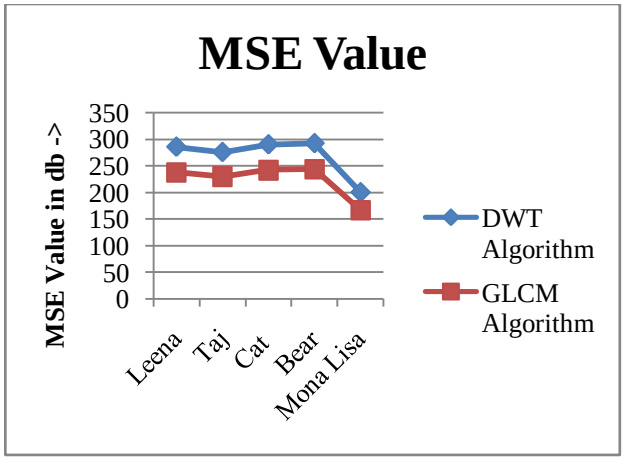

Fig 8: MSE Compassion

As shown in figure 8, the MSE values of proposed and existing algorithms are compared for the performance analysis. It is analyzed that MSE of proposed algorithm is less as compared to existing algorithm which means quality of watermark image is quality.

Table 4: BER Comparison

Image	**DWT Algorithm**	**GLCM Algorithm**
Leena	160.08	10.95
Taj	35.23	24.77
Cat	56.06	3.94
Bear	61.04	1.04
Mona Lisa	71.91	11.91

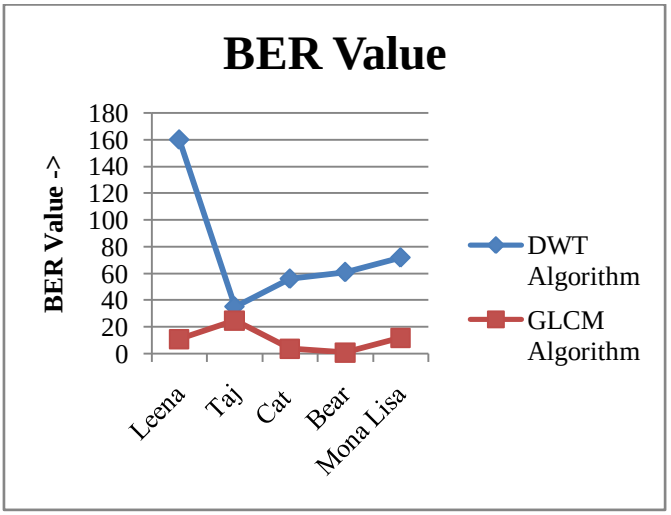

Fig 9: BER Comparison

In the figure 9, it is illustrated BER rate of the proposed and existing algorithm. The BER rate of proposed algorithm is low as compared to existing algorithm

CONCLUSION

In this work, it is concluded that watermarking is the scheme which provide security to the sensitive images. The DWT is the algorithm which selects the bit manually for the watermark image generation. The GLCM algorithm is applied in this research work which selects the embedding bit automatically for the generation of watermark image. The proposed scheme is implemented in MATLAB and compared with existing scheme in terms of PSNR, MSE and BER. It is analyzed that approximate 10 to 15 percent results are improved by applying GLCM algorithm for the bit selection. In future, the key generation scheme will be discovery for the image encryption.

REFERENCES

1. A. M. Zeki, A. A. Manaf, C. F. M. Foozy, and S. S. Mahmod, "A Watermarking Authentication System for Medical Images," presented at the World Congress on Engineering and Technology (CET 2011), Shanghai, China, 2011.
2. R. F. Olanrewaju, O. O. Khalifa, A.-H. Hashim, A. M. Zeki, and A. A. Aburas"Forgery Detection in Medical Images Using Complex Valued Neural Network (CVNN)," Australian Journal of Basic and Applied Sciences, 2011.
3. A. Bamatraf, R. Ibrahim, and M. N. B. M. Salleh" Digital watermarking algorithm using LSB," in Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference on, 2010, pp. 155-159.
4. A. M. Zeki, A. A. Manaf, and M. Zamani, "Bit-Plane Model: Theory and Implementation," in Engineering Conference (EnCon) 2010.
5. Zigang Chen, Lixiang Li, HaipengPeng, Yuhong Liu, and Yixian Yang, “A Novel Digital Watermarking based on General Non-negative Matrix Factorization”, 2018, IEEE, Volume: 20 , Issue: 8, Page s: 1973 – 1986

6. Shuai Liu, Zheng Pan, Houbing Song, "Digital image watermarking method based on DCT and fractal encoding", IET Image Process., 2017, Vol. 11 Iss. 10, pp. 815-821
7. Nasrin M. Makbol, Bee EeKhoo, Taha H. Rassem, "Block-based discrete wavelet transformsingular value decomposition image watermarking scheme using human visual system characteristics", 2016, The Institution of Engineering and Technology-IET Image Process., pp. 1–19
8. BaharakAhmaderaghi, FatihKurugollu, Jesus Martinez Del Rincon and Ahmed Bouridane, "Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory", 2018, IEEE, Volume: 4, Issue: 1, Page s: 46 – 59
9. FerdaErnawan, and Muhammad NomaniKabir, "A Robust Image Watermarking Technique with an Optimal DCT-Psychovisual Threshold", 2018, IEEE, Volume: 6, Page s: 20464 – 20480
10. Chia-Sung Chang and Jau-JiShen, "Features Classification Forest: A Novel Development that is Adaptable to Robust Blind Watermarking Techniques", 2017, IEEE, Volume: 26 , Issue: 8, Page s: 3921 – 3935
11. Nazeer Muhammad, NargisBibi, "Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain", IET Image Process., 2015, Vol. 9, Iss. 9, pp. 795–803
12. Hukum Singh, "Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain", IET Image Processing, 2018, , Vol. 10, Iss. 12, pp. 840–880
13. DeepayanBhowmik, Matthew Oakes and CharithAbhayaratne, "Visual Attention-based Image Watermarking", IEEE ACCESS, 2016, , Vol. 17, Iss. 11, pp. 800–830
14. Abhilasha Singh, Malay Kishore Dutta, "Lossless and Robust Digital Watermarking Scheme for Retinal Images", 2018, 4th International Conference on Computational Intelligence & Communication Technology (CICT), Pages: 1 – 5
15. SubratoBharati, Mohammad AtikurRahman, SanjoyMandal, PrajoyPodder, "Analysis of DWT, DCT, BFO & PBFO Algorithm for the Purpose of Medical Image Watermarking", 2018, International Conference on Innovation in Engineering and Technology (ICIET), Pages: 1 - 6
16. Nasir N. Hurrah, Nazir A. Loan, Shabir A. Parah, Javaid A. Sheikh, "A transform domain based robust color image watermarking scheme for single and dual attacks", 2017, Fourth International Conference on Image Information Processing (ICIIP), Pages: 1 – 5
17. ImaneAssini, AbdelmajidBadri, Khadija Safi, Aicha Sahel, Abdennaceur Baghdad, "Hybrid multiple watermarking technique for securing medical image using DWT-FWHT-SVD", 2017, International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Pages: 1 – 6
18. HansaMehra, SilviyaChouhan, Rita Choudhary, "Forgery resistant image watermarking technique using discrete cosine transform (DCT)",2017, Fourth International Conference on Image Information Processing (ICIIP), Pages: 1 – 5
19. R. Surya PrakasaRao, P. Rajesh Kumar, "An efficient genetic algorithm based gray scale digital image watermarking for improving the robustness and imperceptibility",2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Pages: 4568 – 4571
20. DhekraEssaidani, HasseneSeddik, Ezzedine, Ben Braiek, "Robust and blind watermarking approach based on modified Delaunay triangulation", 2016, 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Pages: 16 – 20

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication