INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

IMPROVED AES AND DES FOR TEXT WATERMARKING IN DOCUMENTS

Gagandeep Kaur, Sukhwinderbir Bhagat
Student:Department of Computer Science, Prof:department of Computer Science
Beant College of Engineering and technology, Gurdaspur,India
gagan2740@yahoo.co.in

ABSTRACT

With secure communication of information over public networks is one of the most imperative challenges. Mutually all the accomplishments to protect texts as well as to break security are quiet popular. With the intention of reduction in the probabilities of attacks, security necessities on the way made to be undetectable. The requirements to reserve ownership information, originality, as well as integrity of text files in such a way which could possibly not be able to acknowledged via everyone is in actuality felt badly. Watermarking of the text files is an important step in the direction of accomplishing these objectives. Nevertheless, to watermark a simple text file (ASCII) in such a way in which the original text will not transform (and it would possibly be quiet problematic to break it), is a big challenge. We have established a novel encoding which can be utilized to insert data in plain text deprived of changing the text file and decoding scheme which can be utilized to extract data from plain text without changing the text file. A system has been established based upon this scheme which includes AES algorithm as well as DES algorithm. This paper describes the system and demonstrates its workings in MATLAB environment.

KEYWORDS Text Watermarking, AES, DES, Encryption, Security

1. INTRODUCTION

Watermarking is a branch of data concealing which is utilized to cover up extra data in computerized media like picture, sound, feature, or content. Computerized watermarking strategy alludes to the procedure of installing the given watermark data, (for example, possession data, name, logo, signature, and so on.) in the defensive data, (for example, picture, sound, feature, or content) and picking the given watermark data from the defensive data, which in not saw by human perceptual framework [1]. As it were, watermarking is a procedure of inserting a computerized signal or watermark containing data remarkable to the copyright proprietor in the article (content, picture, sound, or feature) which is expected to be ensured. An advanced watermark is characterized as an unmistakable or undetectable ID code that is for all time inserted in the information, to transmit concealed information. It stays introduce in the information even after the decoding technique. It is quite often than not giving patent insurance of licensed innovation. The watermark is later used to recognize the accepted copyright proprietor of the article.

1.1 TYPES OF WATERMARKING

i. Public/blind watermarking

When the original data is not needed during the detection process when detecting a mark, that watermark is considered to be blind/public. The solitary thing mandatory is the data utilized to create the watermark initially, similar to a key which might've been utilized as a portion of the procedure to find out the actual watermark for a photograph.

i. Private/non-blind watermarking

The unique information as well as the private keys is essential throughout the discovery procedure, it's deliberated to remain a *private* or *non-blind* watermarking.

ii. Asymmetric/public-key watermarking

In this, neither the unique information, nor a private key is compulsory for the period of the recognition procedure, it's deliberated to be present as an asymmetric/public-key watermarking. Private Key is mostly used to construct the sign, but then again individually a public key is needed to validate the watermark (exactly like how a digital signature is checked in cryptography).

1.2 TYPES OF DATA TO WATERMARK

1. **Picture**

Watermarking a picture is one of the digital data that can be watermarked. A simple algorithm may flip the last bit of data representing each pixel in each photograph. Therefore, the picture will utmost likely not be conspicuously dissimilar as of the unique pictures in cealtering any of blue’s, red, or green, smallest significant bit will not impact the picture all that ample. This is applying a watermark in the direction of a spatial domain.
There’s another method of enhancing a watermark by way of adding it to a frequency domain. For instance, an individual may possibly create pictures which go by various alterations similar to Fast Fourier Transform in advance on applying some watermark, and then prepare a transposed transformation to acquire the actual picture.

2. **Video**

Video watermarking is basically similar to watermarking a picture in spite of everything; videos are prepared of frames of multiple pictures. On the other hand, supplementary refined effects can possibly be done to prevent attacks because video files have another domain a picture may not have temporal domain. One can perhaps add the frame number or a time of the video shoot into the frame such that if the frame is out of order or is misplaced some data, then it turn out to be very evident to the owners.

3. **Audio**

Ever since songs as well as harmony can possibly be copyrighted legitimately, easily by now, audio watermarking has to do furthermore work by way of delivery of the content or for searching of the content. For example, if an online store name is embedded unnoticeably into a music file, FBI, when conducting some major illegal-audio-distribution bust, may be able to trace to the original person the theft started from someone may have bought one song, which he uploaded to an illegal website, which was used to massively distribute.

2. RELATED WORK

Q. Li (2008) [2] presents a novel text watermarking technique but for the Chinese text merely. In his or her method he's mentioned this some bitstream pattern of the text on the basis of which the merging can be done .His approach also describes the pictographic approach of the text and the visual potential of the person. This method will be despite the fact that comes with a usefulthinking but the problem is as the Chinese language is so sophisticated, it fits there but not with each and every terminology. His / her algorithm may be intended particularlyfor Chinese characters and hence this algorithm cannot be used for global language. Z.Jalil et al. (2010) [3] presented a zero text watermarking scheme in the international conference of 2010. According to them, existing text watermarking algorithms are not robust against random insertion and deletion attacks on particular text document. By means of growing volume of attack, the existence of watermark in the text document turn out to be challenging and hence they developed a novel text watermarking algorithm that can be used for copyright protection of textual materials. They will when matched their results along with various other existing algorithms of the same contrast and their results are found to be effective enough to get proceeded for modification. M. Mali (2013) [4] presented a watermarking scheme on the basis of NEURAL networks. It was a fantastic idea to introduce Neural Networks into the contrast associated with encryption. The Neural Network produces weight for each and every input provided to it rather than taking everything as an input stream. The pattern changing of neural network is quite similar to SVM as it also converts the entire input according its simplification and then proceeds Hence his method is quite effective and can be considered for future development process. N.Divecha (2013) [5] presented a watermarking scheme based on the wavelet quantization method which is again an appreciable effort in this filed. DWT stands for Discrete Wavelet Transformation and it converts the entire data scenario into waves. Preceding the texts as wave is a unique method in this type of enactment. The time and effort accomplished simply by Nidhi had only one negative aspect , she did not mention the type of wavelet transformation she is using as there are a lot of wavelet transformation like Dabuchi, Symlet and others and hence her method can be tried with the above mentioned wavelet family members. F.Alam (2013) [6] introduced the concept of signature in his scheme of watermarking. The signature structure is little bit alike to the private and public key concept in which the public key is visible to all but it requires a private key to change to unlocked. If this technique is experimented underneath invisible watermarking concept, it is fine but if it is used as a visible watermarking concept, the motive of hiding of data remains untouched as the user would be able to identify easily that some data is hidden behind the encrypted text. F. HARTUNG (1999) [7] Multimedia watermarking technology has evolved very quickly during the last couple of decades. A digital watermark is data which is imperceptibly and robustly embedded in the host data such that it could not possibly be detached. A watermark usually encompasses data about the source, status, or person of the host information. In this tutorial paper, the necessities and applications for watermarking are studied. Applications consist of copyright protection, data monitoring, and information tracking. The basic concepts of watermarking systems are outlined and illustrated with proposed watermarking methods for video, text documents, pictures, audio, and also other media. Robustness along with security characteristics are deliberated in greater detail. In conclusion, several remarks are designed around the state of the art and possible future developments in watermarking technology. M.Barni (1998) [8] Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia data in a networked environment. It makes possible to tightly associate to a digital document a code allowing the identification of the information initiator, possessor, approved customer, and so forth. In this document, a brand new watermarking procedure for digital pictures is displayed: the tactic that performs in the frequency domain embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. After embedding, the watermark is adapted to the picture by exploiting the masking characteristics of the human graphic system, therefore confirming the watermark hiddenness. By discovering the statistical assets of the embedded order, the sign can be dependably removed deprived of resorting to the original uncorrupted picture. Trial results display the watermark is robust to several signal processing techniques, including JPEG compression, low pass and median filtering, histogram equalization and stretching, dithering, addition of Gaussian noise, resizing, and multiple watermarking. J.Hernández (2000) [9] In his work, a new spread-spectrum-like individually distinct cosine transform domain (DCT domain) watermarking technique for copyright protection of still digital pictures are investigated. The DCT is executed in blocks of 8 × 8 pixels as in the JPEG procedure. The watermark can encrypt data on the way to track illegitimate misuses. For flexibility commitments, the unique picture is not necessary during the ownership verification procedure, so it need to be demonstrated by noise. Double tests are involved in the proprietorship verification stage: watermark deciphering, that the message carried with the watermark will be removed, along with the watermark discovery that chooses no matter if a given picture contains a watermark generated with a definite key. They utilize generalized Gaussian distributions to statistically model the DCT coefficients of the original picture and show how the resulting detector structures lead to considerable improvements in performance with respect to the correlation receiver, that has recently been broadly thought to be in the literature and makes use of the Gaussian noise assumption. Accordingly to their work, analytical terminologies for performance measures such as the probability of error in watermark decoding and probabilities of false alarm and detection in watermark detection are derived and contrasted with experimental results. V.Santhi et al. (2009) [10] have presented the advancement in Computer technology and readily accessible tools; it is quite simple for the unfamiliar users on the way to produce illegal copies of multimedia data which are floating across the Web. With the purpose of protecting those audio-visual aid information on the Internet many techniques are available including various steganography methods, encryption methods, information covering methods, and watermarking methods. Digital watermarking is a method that a piece of digital information is embedded into a picture and extracted later for ownership authentication. Top-secret digital information could possibly be implanted more over in spatial domain or in frequency domain of the cover information. In this paper, a different singular value decomposition (SVD) and discrete wavelet transformation (DWT) based technique is proposed for hiding watermark in full frequency band of color pictures (DSFW). The quality of the watermarked picture and extracted watermark is measured using peak signal to noise ratio (PSNR) and normalized correlation (NC) correspondingly. It is witnessed that the superiority of the watermarked picture is maintained with the worth of 36dB. Robustness of proposed algorithm is verified for various attacks including salt and pepper noise and Gaussian noise, JPEG compression setting along with cropping. P.Cheema et al. [11] have presented a technique components of English terminology including noun, pronoun, model verbs along with conjunctions associated with user's choice along with author id are used to create watermark of user's choice. Moreover, encryption techniques AES algorithm is applied to encrypt watermark and to enhance its security level to protect it from tampering attacks and to prove the most robust algorithm. B.Saha et al. (2014) [12] has presented a robust watermarking algorithm using DES, ECC and DCT for color pictures. The original color picture (watermark) and cover picture has been separated into three independent color channels (red, green and blue) and their gray scale equivalents are used. Each individual gray scale equivalent of RGB components of original picture has been encrypted using Data Encryption Standard (DES). The Henon map is used to generate three different round keys for DES with different initial parameters. L.Ling et al. (2010) [13] has presented a watermarking scheme based on DCT transform by Arnold map and spread spectrum which is proved to be robust and secret in nature. The Arnold transformation has been used to encrypt the watermark picture. Resulting encrypted picture is embedded into DCT coefficient which is selected by spread spectrum.

3. PROBLEM STATEMENT

As going through all the previous work, we come to know that the importance of hiding data in encrypted form is highly required in all manners for the global world communication. In one of the latest work done by "Markand L Mali " an extended scheme using AES Algorithm has been presented in the international conference of 2013. His work is highly appreciable and it gives birth to our problem statement. If we perform a single level encryption mechanism for the text, it would become a little easier for the decrypted end to make it visible to the user and hence a question can be put on the standard of encryption. Our problem is to combine the AES Algorithm with DES algorithm for hidden watermark. The parameters of the comparison can be the time taken to decrypt the content.

4. PROPOSED TECHNIQUE

Step 1 : First, we should take the plain text.

Step 2 : Then we will call AES algorithm which would generate two keys namely private key and the public key.

Step 3 : Then the public key would be provided to the DES Algorithm which would encrypt the already encrypted text and hence a dual encryption would be performed.

Step 4 : Then after this procedure it would be watermarked.

Step 5 : By the time of decryption, first the inverse DES would be required to generate the public key of the AES algorithm

Step 6 : And afterwards according to the document, the private key of the document would be called to decrypt the entire content.

Step 7 : In the end, we will evaluate the results based on PSNR and MSE parameters.
The parameters of the judgment would be as follows.

A) **PSNR:** Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

B) **MSE:** In statistics, the mean squared error of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.

5. PROPOSED ALGORITHM

The text watermarking calculation comprises of four sections: the watermark, the encoder (insertion calculation), the finder and the comparator (confirmation or extraction or location calculation) [10].

It expect a unique content record O, a mystery key K=k1, k2,…ki, watermark M and the watermarked content report W. Watermark M is inserted after the key. The insertion capacity E produces a watermarked content record T' compare to the info of O, M and K. The capacity E is spoken to by

E (O, K, M) = W [1]

The identifier capacity D takes a content record (H is an associated unlawful content archive with O. H is at any rate looks like O) and copyright proprietor's key K = k1, k2,…ki then it extricate watermark M'. The capacity D is spoken to by D (H, K) =M' [2]

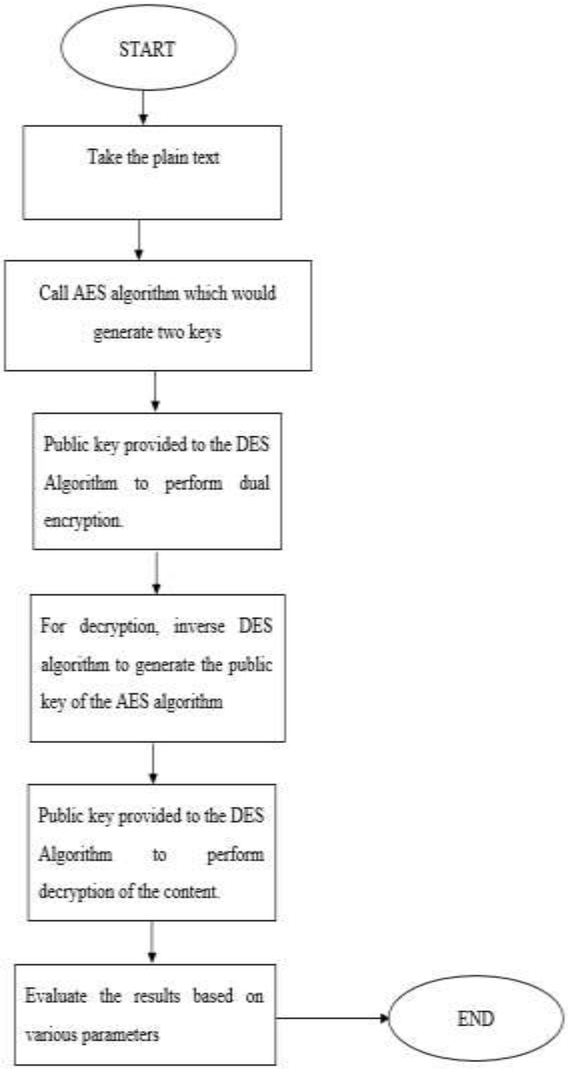
START
Take the plain text
Call AES algorithm which would generate two keys
Public key provided to the DES Algorithm to perform dual encryption.
For decryption, inverse DES algorithm to generate the public key of the AES algorithm
Public key provided to the DES Algorithm to perform decryption of the content.
Evaluate the results based on various parameters
END

Figure 1 Flow chart of proposed work

A look at capacity C takes M' as an info to contrast and all M recorded in its framework information base.

C (M’, M) = 1; if M’=M, generally C (K’, K) =0 if M’≠M.

The accompanying figure outlines over three capacities and the entire content watermarking calculation. Accept it is in the advanced library situation.

6. EXPERIMENTAL SET UP AND RESULTS

In order to implement the proposed algorithm, design and implementation has been done in MATLAB using image processing toolbox. The developed approach is compared against some well-known image watermarking techniques available in literature. In order to do cross validation we have also implemented a new semi-blind watermarking scheme based on discrete wavelet transform (DWT) and subsampling. After these comparisons, we are comparing proposed approach against Gaussian Noise, Median Filtering and Histogram Attack using some performance metrics. Result shows that our proposed approach gives better results than the existing techniques. Table 1 is showing the various images which are used in this research work. Images are given along with their formats. All the images are of same kind and passed to proposed algorithm.

Table 1 Images taken for experimental analysis

Image name	Extension	Water mark	Extension
Hydrangeas	.jpg	1	.jpg
Strawberries	.jpg	Logo1	.png
Cake	.jpg	Logo2	.png
Pomegranate	.jpg	Adesh	.jpg
Chrysanthemum	.jpg	Punjabi	.jpg
Baby	.jpg	Arrows	.jpg
Sunset	.jpg	Water	.jpg
Sea	.jpg	Dds	.jpg
Warning	.jpg	Hello	.jpg
Sparrow	.jpg	Star	.jpg

The proposed algorithm is tested on various images. The algorithm is applied using various performance indices Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Bit Error Rate (BER), and Root Mean Square Error (RMSE).

In order to implement the proposed algorithm, design and implementation has been done in MATLAB using image processing toolbox. In order to do cross validation we have also implemented semi blind watermarking scheme using DWT-sub sampling. The developed approach is compared against some well-known watermarking techniques available in literature. After these comparisons, we are comparing proposed approach against Gaussian Noise Attack, Median Filter Attack and Histogram Attack using some performance metrics. Result shows that our proposed approach gives better results than the existing techniques.

The whole simulation has been taken place in MATLAB environment using various parameters like: PSNR and MSE.

1. **PSNR:** The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$\text{PSNR}=10*\log(255*255/\text{MSE}) \qquad \text{eq.1}$$

2. **MSE:** The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is

$$\text{MSE} = \frac{1}{mn} \sum \sum [(I,j) - K(I,j)]^2 \text{eq.2}$$

where M and N are the number of rows and columns in the input images respectively.

Case.1 for Image 1

Above figure.2 shows the cover image that has to be taken for watermarking and figure.3 shows the watermarking image that has been showed in which watermarking of text is done by encryption algorithms AES and DES

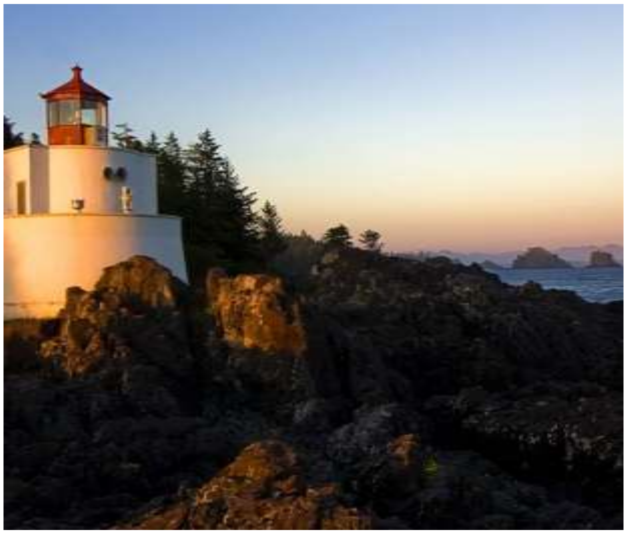

Figure.2 Input Cover Image

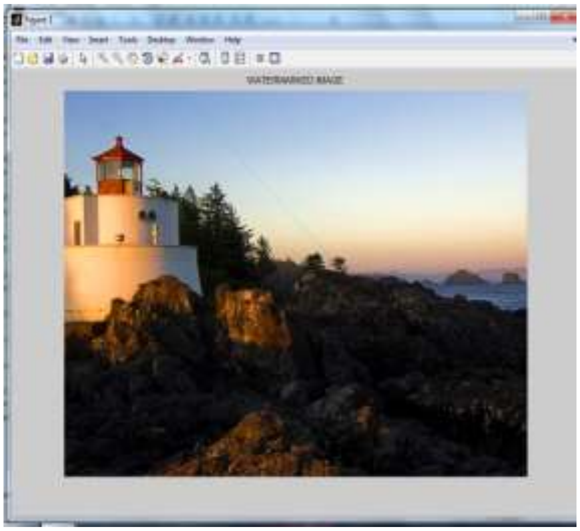

Figure. 3 Watermark Image

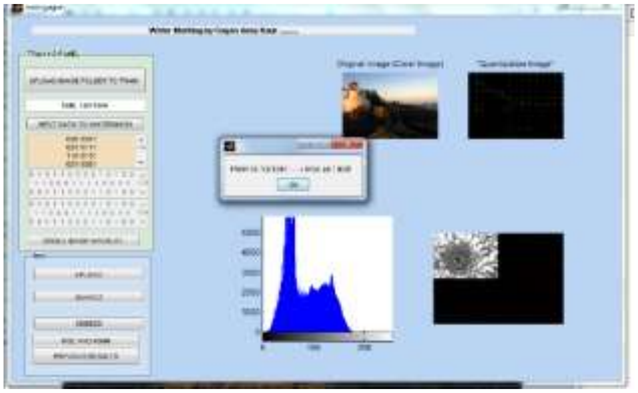

Figure.4 PSNR and MSE value for proposed method

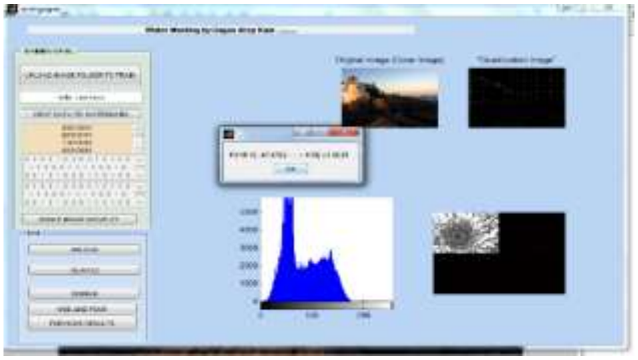

Figure.5 PSNR and MSE value for previous method

Above figure.4 and Figure.5 shows the value of PSNR and MSE for proposed method and base method respectively and it has been shown that proposed method has good values for both PSNR and MSE parameters.

Case.2 for Image 2

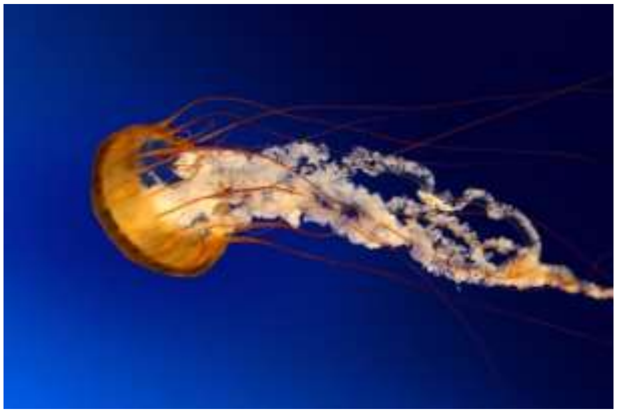

Figure.6 Input Cover Image

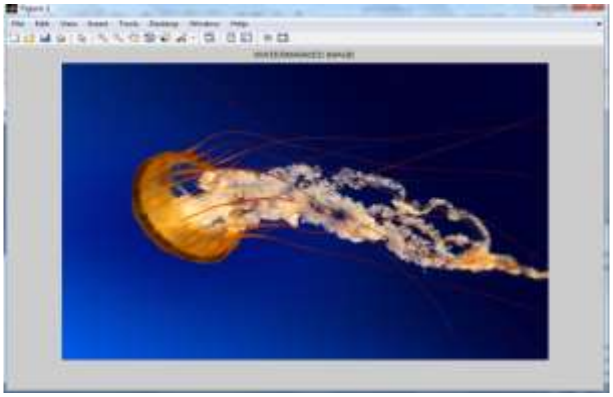

Figure. 7 Watermark Image

Above figure.6 shows the cover image that has to be taken for watermarking and figure.7 shows the watermarking image that has been showed in which watermarking of text is done by encryption algorithms AES and DES.

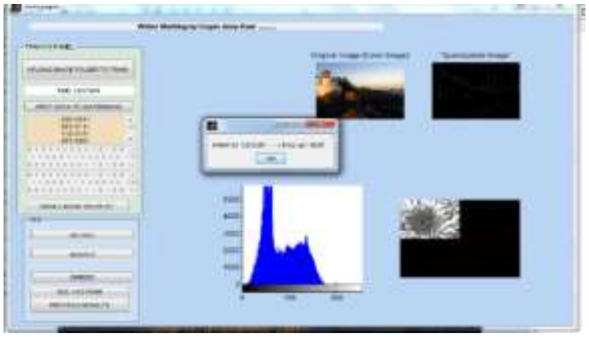

Figure.8 PSNR and MSE value for proposed method

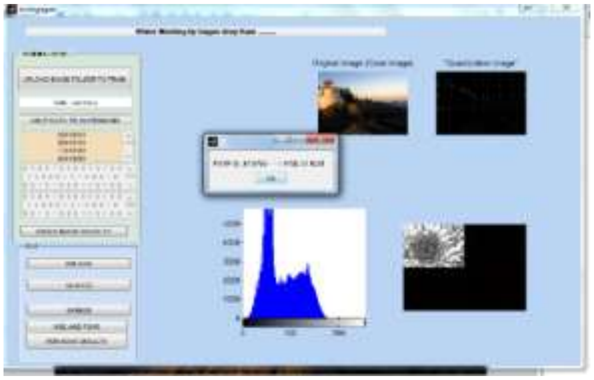

Figure.9 PSNR and MSE value for previous method

Above figure.8 and Figure.9 shows the value of PSNR and MSE for proposed method and base method respectively and it has been shown that proposed method has good values for both PSNR and MSE parameters.

7. PERFORMANCE ANALYSIS

This section contains the cross validation between existing and proposed techniques. Some well-known image performance parameters for digital images have been selected to prove that the performance of the proposed algorithm is quite better than the existing methods.

Mean Square Error Evaluation

Table 2 is showing the quantized analysis of the mean square error. As mean square error need to be reduced therefore the proposed algorithm is showing the better results than the available methods as mean square error is less in all the cases.

Table 2 Mean Square Error Evaluation

Images	Water mark	Existing Technique	Proposed Technique
Hydrangeas	1.jpg	0.7929	0.6637
Strawberries	1.jpg	0.9385	0.7535
Cake	1.jpg	0.3674	0.3287

Pomegranate	1.jpg	0.8256	0.6953
Chrysanthemum	1.jpg	0.8198	0.6535
Baby	1.jpg	0.5285	0.3515
Sunset	1.jpg	0.8611	0.6853
Sea	1.jpg	0.1068	0.0392
Warning	1.jpg	0.6056	0.5697
Sparrow	1.jpg	0.7590	0.7465

Figure 10 has shown the quantized analysis of the mean square error of different images using watermarking by Existing Technique (Red color) and watermarking by Proposed Approach (Blue Color).

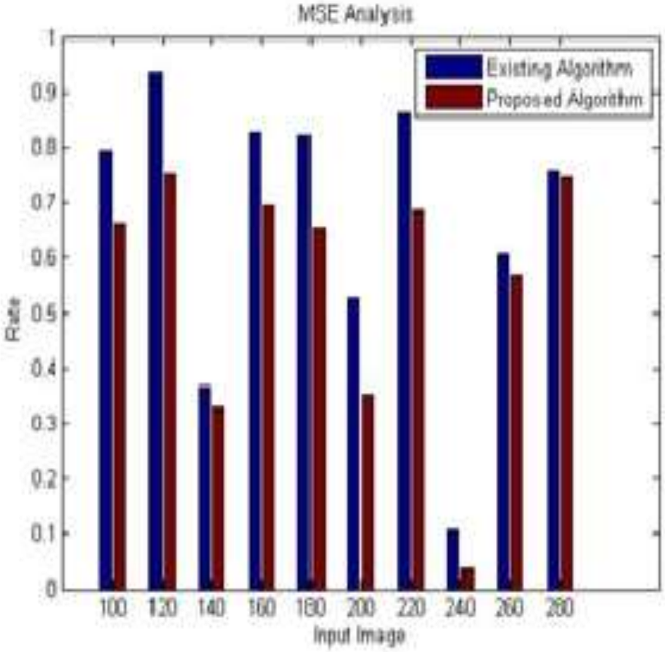

Figure 10: MSE of Existing Technique & Proposed Approach for different images

It is very clear from the plot that there is decrease in MSE value of images with the use of proposed method over other methods in all images. This decrease represents improvement in the objective quality of the image.

Peak Signal to Noise Ratio Evaluation

Table 3 is showing the comparative analysis of the Peak Signal to Noise Ratio (PSNR). As PSNR need to be maximized; so the main goal is to increase the PSNR as much as possible. Table 3 has clearly shown that the PSNR is maximum in the case of the proposed algorithm therefore proposed algorithm is providing better results than the available methods.

Table 3 Peak Signal to Noise Ratio Evaluation

Images	Water mark	Existing Technique	Proposed Technique
Hydrangeas	1.jpg	37.7691	49.9108
Strawberries	1.jpg	37.2062	48.3497
Cake	1.jpg	40.3370	52.9625
Pomegranate	1.jpg	37.6342	49.7092
Chrysanthemum	1.jpg	37.6578	45.2531
Baby	1.jpg	39.1233	52.6718
Sunset	1.jpg	37.4936	46.4523
Sea	1.jpg	44.4616	62.2004
Warning	1.jpg	38.6684	50.2976
Sparrow	1.jpg	37.9151	49.4005

Figure 11 has shown the quantized analysis of the peak signal to noise ratio of different images using watermarking by Existing Technique (Red Color) and watermarking by Proposed Approach (Blue Color).

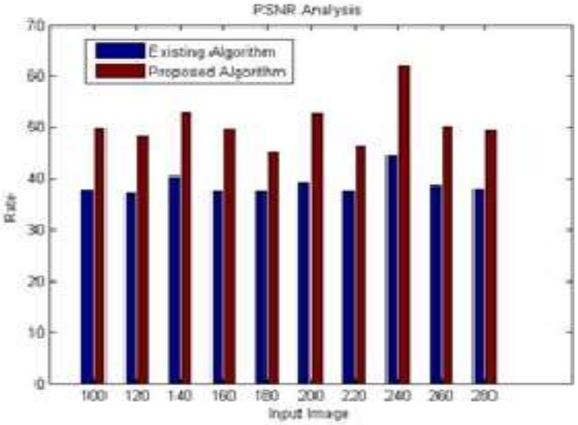

Figure 11: PSNR of Existing Technique & Proposed Approach for different images

It is very clear from the plot that there is increase in PSNR value of images with the use of proposed method over other methods. This increase represents improvement in the objective quality of the image.

8. CONCLUSION

Encryption algorithm plays an important role in communication security where encryption time, Memory usages and battery power are the major issue of concern. The selected encryption AES and DES algorithms are used for performance evaluation. Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption time compare to DES. When data size increases then asymmetric cryptographic algorithm performs slower compare to symmetric algorithm. In this paper, similar algorithms have been used for all text categories. Algorithms can be designed specific to the text category and optimum parameter setting can be proposed for text categories like SST, MST, LST and VLST. Hand written text, manual signatures, and fingerprints can also be taken as watermark and further experiments can be conducted on these.

REFRENCES

[1] Robert, L., and T. Shanmugapriya, *A Study on Digital Watermarking Techniques,* International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[2] Qing-Cheng Li “Novel Text Watermarking Algorithm based on Chinese Characters Structure 2008 International Symposium on Computer Science and Computational Technology

[3] “Zunera JaliI, Hamza Aziz Saad Bin Shahid\ Muhammad Arif “A Zero Text Watermarking Algorithm based on Non-Vowel ASCII Characters 978-1-4244-8035-71101$26.00 © 2010 IEEE

[4] Makarand L. Mali “Implementation of Text 2013 International Conference on Communication Systems and Network TechnologiesWatermarking Technique Using Natural Language Watermarks

[5] “NidhiDivecha” Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color pictures 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)

[6] ” Fahim Irfan Alam “An Investigation into picture Hiding Steganography with Digital Signature Framework 978-1-4799-0400-6/13/$31.00 ©2013 IEEE

[7] FRANK HARTUNG,” Multimedia Watermarking Techniques”, 0018–9219/99$10.00 ã 1999 IEEE PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999

[8] Mauro Barni,” A DCT-domain system for robust picture watermarking”, Signal Processing 66 (1998) 357Ð372

[9] Juan R. Hernández,” DCT-Domain Watermarking Techniques for Still pictures: Detector Performance Analysis and a New Structure”. IEEE TRANSACTIONS ON PICTURE PROCESSING, VOL. 9, NO. 1, JANUARY 2000

[10] V.Santhi,” DWT-SVD Combined Full Band Robust Watermarking Technique for Color pictures in YUV Color Space”, International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009 1793-8201.

[11] Prabhjot Kaur Cheema1, Kamaljit Kaur2, “Comparison of Text Watermarking Approaches with the Proposed Approach Based on Encryption Techniques used for Creating Watermarks”

[12] BidyutJyotiSaha, Kunal Kumar Kabi, Arun and Chittaranjan Pradhan, “A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color pictures” 2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT]

[13] Lu Ling, Sun Xinde, CaiLeiting, “A robust watermarking based on DCT by Arnold transform and spread spectrum,” *3rd international conference on advanced computer theory and engineering, IEEE,* Vol. 6, 2010, pp. 198-201

.