

A Hybrid DWT-SVD-PCA Model for Robust and Encrypted Image Watermarking

Margaret Katherine Williams^{*1} & Er. Samuel Stephen Dawson²

^{*1} Assistant Professor, Brighton Mechanical and Civil Engineering College, Brighton, UK

ABSTRACT

A watermark is a form of image or text that is impressed onto the paper that provides evidence of its authenticity. Although various watermarking techniques have been developed studied in literature and it's a valuable tool for copyright protection, information hiding and data integrity. Watermarking may be done in spatial domain or transform domain such as DCT or wavelet. We choose to insert the mark in DWT domain because this is domain still used by many algorithms and have advantages over DCT standard. We use DES algorithm to encrypt the watermark image and transform ciphers are used to transform the text watermark. This method is useful to achieve certain level of quality. The performance of our proposed system is evaluating by calculating PSNR and MSE values of original and watermark image. The results prove that the algorithm is robust enough to handle the various types of attacks. Our system can preserve the appropriate level of quality. By embedding the watermark into DWT is far better than embedding the watermark in DCT domain. The Proposed research aims to develop an improved Watermarking approach which is based on DWT and SVD along with encryption. Of color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks. Images as well as text messages can be hide within the images using sequential and random methods. It will incorporate cryptography to achieve high security and random pixel embedding to attain high immunity to attacks. Performance of the same had been analyzed by calculating normalized correlation (NC), peak signal to noise ratio(PSNR) men square error (MSE) for various attacks. Moreover the performance of had been compared with Tapas *etal* Algorithm, DSAWM Algorithm. Here we have tested this system on 50 different images. Maximum observed values of the proposed system for PSNR is 68.41 without attaks and 58.94 with attacks. Minimun MSE values of the existing test cases comes out to be 0.0018992. whereas value of NC is evaluated as 0.9984. These values are far better than that of existing systems. In the proposed system a new technique is developed to watermark the images after encryption process. In addition to DES algorithm we use DWT and SVD to apply the watermark. Proposed system is also tested on various types of attacks on the watermarked images to check the robustness of the system.

KEYWORDS: Digital watermarking, Information Hiding, DES , DWT, SVD.

1. INTRODUCTION

The process of embedding information into another object/signal can termed as watermarking. The basic idea of watermarking is embed a stealthy image into the image needed to be secured. The stealthy image is derived from the original image and should carry sufficient information to ensure copyright verification. Cryptography has been the corner stone of technologies used to protect intellectual property rights. However, cryptography protects only the work during transmission or distribution. This provides no protection after the work is decrypted. All work must eventually be decrypted if consumers are to enjoy the photograph, music, or movie. Watermarking is a technology that complements cryptography by embedding imperceptible signals in a work. The signals remain in the work after decryption and even after conversion to analog world, and their use has been proposed for the variety of digital rights management purposes. Thus watermark is a secondary image which overlaid within the primary image and provides way to protect the image.

2. DIGITAL WATERMARKING

Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing the multimedia data. Encryption of the multimedia products prevents an intruder from accessing the contents without a proper decryption key. Digital Watermarking is the process of embedding data called a watermark into the digital media such that watermark can be detected or extracted later to make an assertion about the object.

Digital Watermark Classification

A digital watermark is called robust with respect to the transformations, if embedded information may be detected reliably from the marked signal, even if degraded by any number of the transformations. Typical image degradations may be by JPEG compression, rotation, cropping, noise and quantization of image. A digital watermark is imperceptible if the watermarked content can be perceptually equivalent to the original, unwatermarked content. In general, it is easy to create the robust watermarks or imperceptible watermarks, but the creation of the robust and imperceptible watermarks can prove to be quite challenging. A robust imperceptible watermark has proposed as tool for the protection of the digital content.

Digital watermarking techniques can be classified on following basis:-

- **Robustness**

A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks can be used in a copy protection application to carry copy and no access control information.

- **Perceptibility**

A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable. The digital watermark is called perceptible if its presence in the marked signal is noticeable (e.g. Network Logo, Content Bug, Codes, and Opaque images.) This should not be confused with perceptual which is watermarking which used the limitations of human perception to be imperceptible.

- **Capacity**

The length of the embedded message determines two different main classes of digital watermarking schemes: The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked objects. These kind of watermarking schemes is usually referred to as zero-bit or presence watermarking schemes. Most of the times, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

- **Embedding method**

A digital watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermark is known to be modest robust, but also have a low information capacity due to host interference. The digital watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer with low robustness, but have high information capacity due to rejection of host interference. The digital watermarking method is referred to as amplitude modulation which is similar to spread spectrum method, but is particularly embedded in the spatial domain.

3. LITERATURE SURVEY

Murty et al. (2011) [23] demonstrates DES encryption to the watermark with a key and iterating operations ensure security of the watermark information. If one have to extract the watermark image, one must obtain the secret key. The results show that the watermark is robust against various attacks. In this, digital watermarks and signature method for image authentication is proposed using cryptography analysis. Digital signature created for the original image and then watermark is applied. The Images are resized before transmission into the network. Apply the encryption and decryption process to an image for the authentication, after digital signature and water marking an image. The encryption is used to securely transmit data in open networks and the encryption of an image using public key and decrypt that image using private key.

Kashyap and Sinha (2012) [16] proposed a watermarking technique on robust image for the copyright protection based on 3-level discrete wavelet transform (DWT). In this method, a multi-bit watermark is embedded into the cover image with low frequency sub-band by using alpha blending method. The insertion and extraction of the watermark in the grayscale cover image is found to be simple than other transform methods. The proposed method is compared with the image watermarking methods based on 1-level and 2-level DWT by

using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE). This method embeds the invisible watermark into salient features of the image using alpha blending method.

Perwej et al. (2012) [24] proposed edge detection method using Gabor Filters. In this paper least significant bit (LSB) substitution method is used to encrypt the message in the watermark image file. The LSB does not result in a difference human perceptible because the change in amplitude is little therefore the human eye the resulting stego image will look identical to the cover image and this allows a high perceptual transparency of LSB. The spatial domain technique LSB substitution used a pseudo-random number generator to determine the pixels for embedding based on a given key. The watermarking robustness have calculated using the Peak Signal to Noise Ratio (PSNR) and the Normalized cross correlation (NC) is used to quantify using the similarity between the real watermark and after extracting watermark.

Kaur and Kaur (2013) [18] proposed a LSB Technique based image watermarking has two different parameters Standard deviation and Mean. Image watermarking hide in two ways, either text is used for secret message or image is used for secret image. After selecting the information hiding message, it uses LSB method and hides the information on high result value of these parameters. Watermarking can be used in different techniques to hide the secret image like DCT, DFT, DWT and others. Image Watermarking can be implemented through LSB method. In this research both the text and the image is watermarked using existing LSB method

and the results are analyzed by using different parameters of the image which are used to place the watermark in the original image.

4. METHODOLOGY

The Proposed research aims to develop an improved Watermarking approach which is based on DWT and SVD along with encryption. of color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks. Images as well as text messages can be hide within the images using sequential and random methods. It will incorporate cryptography to achieve high security and random pixel embedding to attain high immunity to attacks. It would be highly immune to any environmental disturbances like noise due to hybrid filtering.

Discrete wavelet transform (DWT)

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet.

DWT is the multire solution description of an image the decoding can be processed sequentially from a low-resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges. In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub- bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band. The three-level DWT decomposition is shown in following diagram:

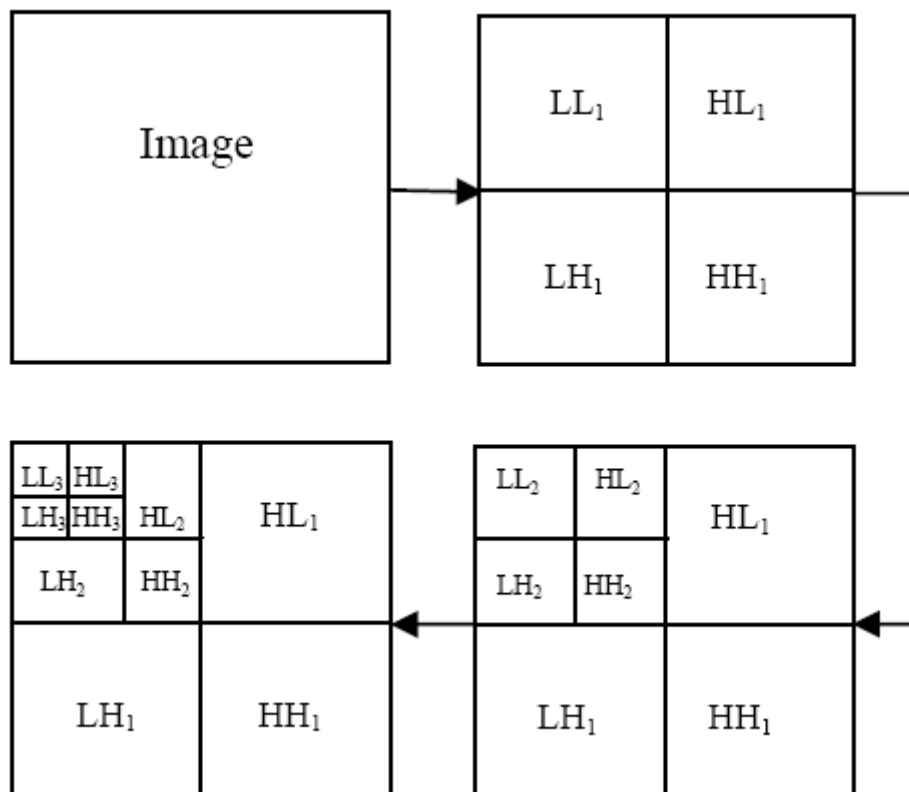


Fig 4.1:3-Level discrete wavelet decompositions

Singular Value decomposition (SVD)

SVD is an effective numerical analysis tool used to analyse matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as the original matrix. From the view point of linear algebra, an image is an array of nonnegative scalar entries that can be regarded as a matrix. Without loss of generality, if A is a square image, denoted as $A \in R^{n \times n}$, where R represents the real number domain, then SVD of A is defined as $A = USV^T$ where U and V are orthogonal matrices, and S is a diagonal matrix, as

$$S = \begin{bmatrix} s_1 & & \\ & \ddots & \\ & & s_n \end{bmatrix}$$

Here diagonal elements i.e. s's are singular values and satisfy $s_1 \geq s_2 \geq \dots \geq s_r \geq s_{r+1} = \dots = 0$ SVD is an optimal matrix decomposition technique in a least square sense that it packs the maximum signal energy into as few coefficients as possible.

The proposed system comprises of two components:

1. Embedding Module
2. Extracting Module.

Algorithm

The proposed system will work as shown below:

Step 1: Input the Cover and watermark image.

Step 2: Perform the three level DWT of cover image.

Step 3: Perform the encryption using encryption key of watermark image using encryption algorithm

Step 4: Perform one level DWT of the encrypted image

Step 5: Now embedded lower frequency sub band of watermark in lower frequency sub band of cover image.

Step 6: Extract the watermark from the step 5.

Step 7: Decrypt the watermark using decryption algorithm along with decryption key.

Step 8: Evaluate the performance of the proposed system on the basis of the performance parameters.

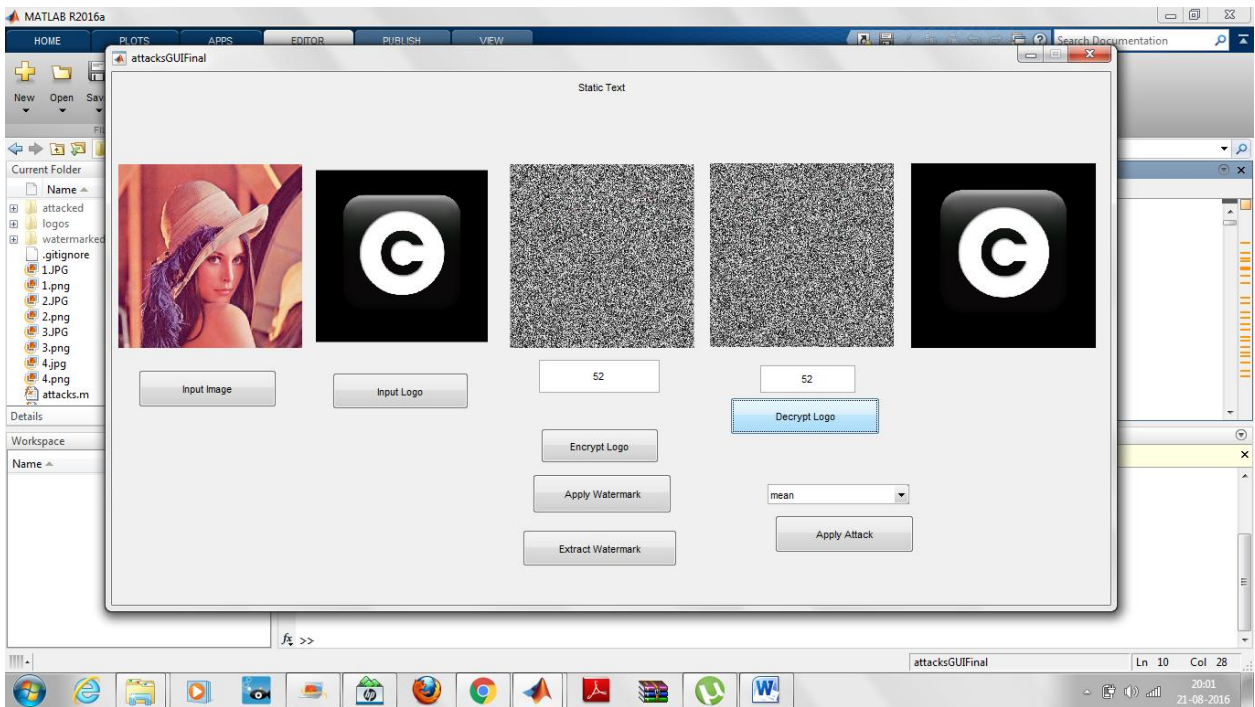
Step 9: Compare the performance parameters of the proposed system with the existing system.

Step 10: Perform the above algorithm to different set of images.

5. EXPERIMENTAL RESULTS AND SIMULATIONS

In this thesis work a digital image watermarking algorithm had been implemented using MATLAB platform. Moreover the performance of proposed algorithm has been compared with Tapas *et al.* and DSAWM algorithm. Snapshot of the Proposed System:

The following is the snapshot of the proposed system










Performance analysis and comparison on various attacks:

Rotation attacks

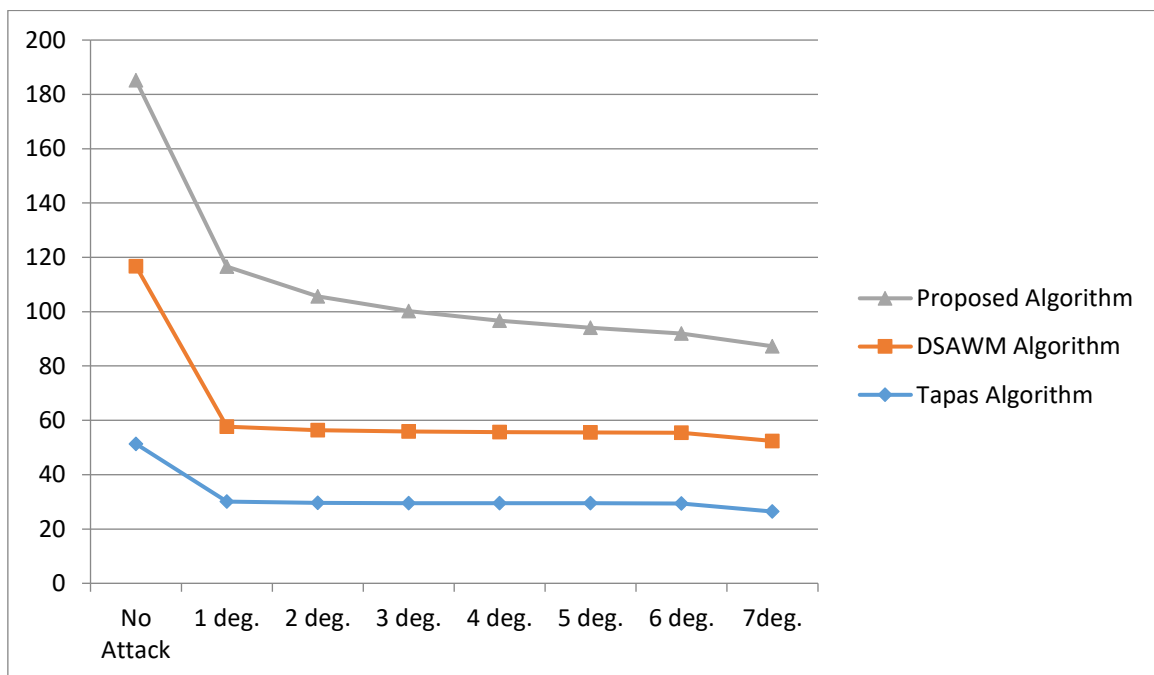
Watermarked image was subjected to rotation attacks. In MATLAB, `imrotate` is the function which is used to rotate the image with different angles. Rotation reduces the correlation among the pixels which affects peak signal to noise ratio, mean square error and cross correlation. Watermarked image is rotated at different angles and its impact is studied.

Table 5.1 Comparison between PSNR, MSE, NC values (Rotation attack)

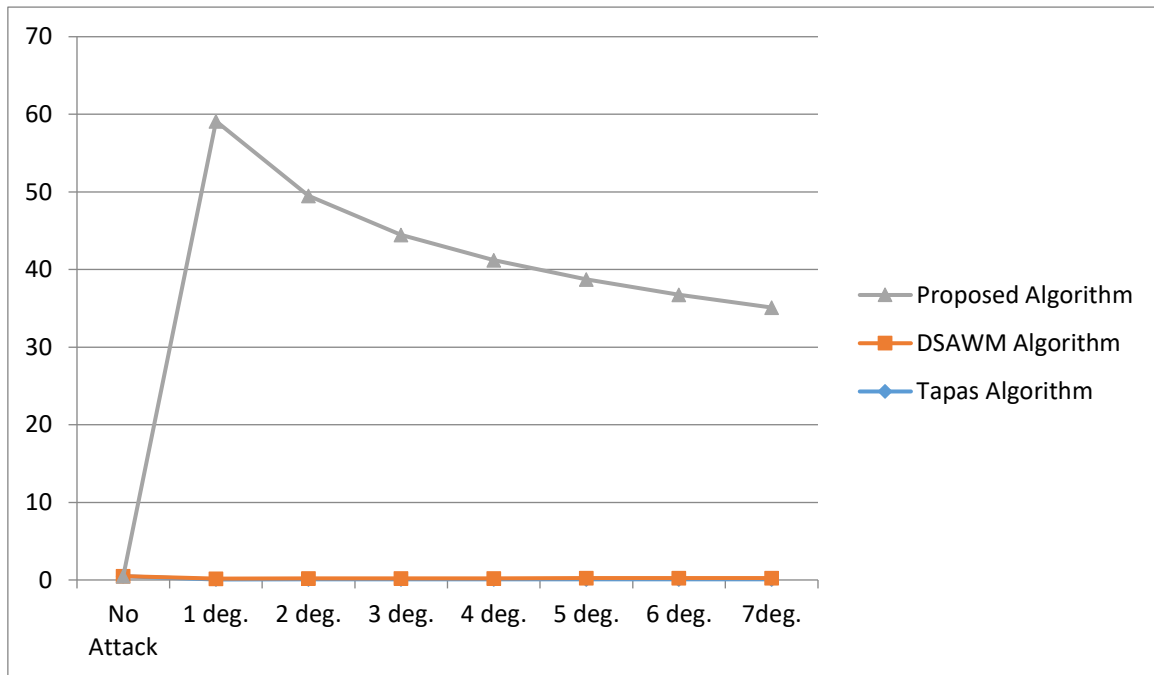
Sr NO.	Rotation attack	Tapas <i>et al</i> Algorithm			DSAWM Algorithm			Algorithm		
		PSNR	MSE	NC	PSNR	MSE	NC	PSNR	MSE	NC
1.	No attack	51.3458	0.476	0.999	65.382	0.0188	1.000	68.4146	0.0052125	1.000
2.		30.114	0.063329	0.735	27.587	0.113322	0.973	58.9411	0.0052124	0.9984
3.		29.660	0.070315	0.609	26.671	0.139938	0.922	49.2776	0.0010448	0.9991
4.		29.529	0.072461	0.529	26.389	0.149311	0.865	44.2414	0.0014979	0.9993
5.		29.485	0.073207	0.475	26.229	0.154922	0.811	40.9725	0.0018992	0.9990

6.		29.442	0.073 925	0.435	26.12 3	0.158747	0.766	38.5205	0.0028657	0.9984
7.		29.424	0.074 246	0.401	26.04 6	0.161595	0.725	36.5101	0.0026183	0.9976
8.		29.4270	0.074 194	0.374	25.99 5	0.163513	0.685	34.8589	0.0029466	0.9965

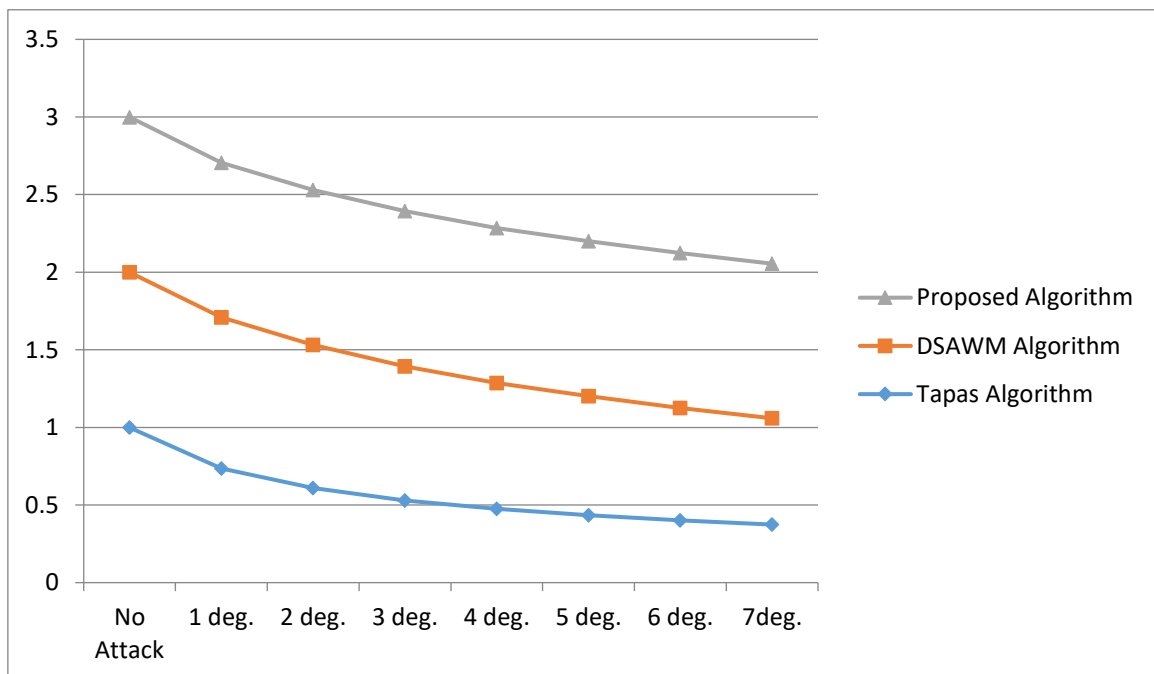
PSNR Comparison Graph for Rotation attack:



MSE Comparison



NC Comparison



Scaling Attack

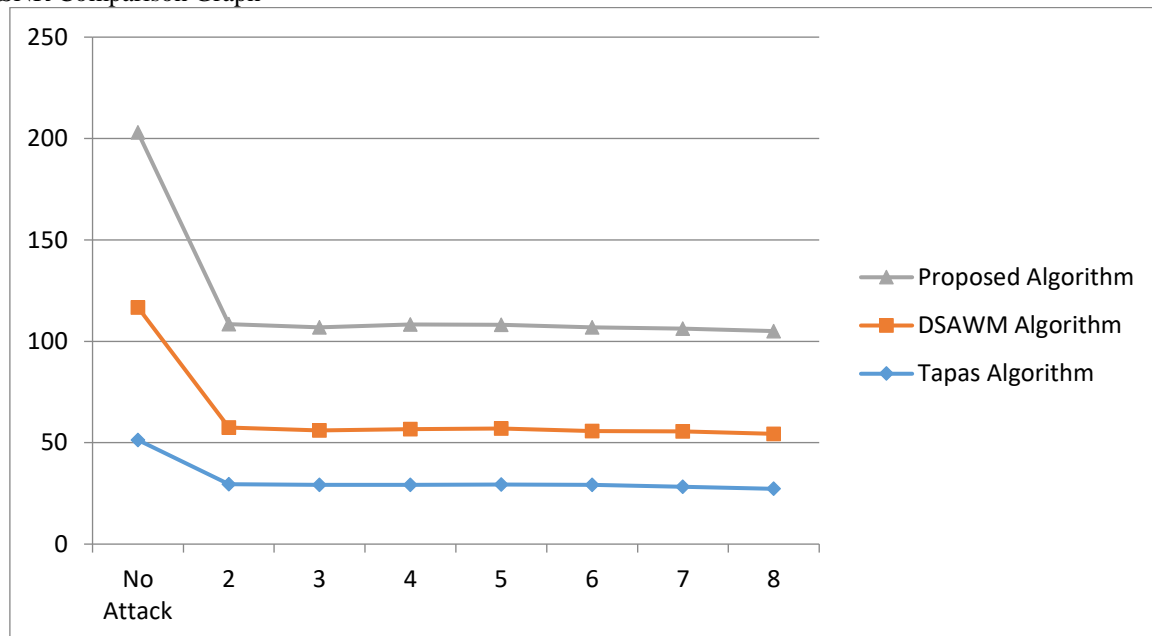
Scaling is a transformation that enlarges or diminishes objects. In other words, scaling points to resizing the image. On resizing the image correlation among the pixels is changed which leads to transformation of image. Watermarked image was subjected to different scaling dimensions attacks. Scaling is a geometric attack like

rotation which tests robustness of the algorithm. Following shows performance analysis of scaling effect on both algorithms.

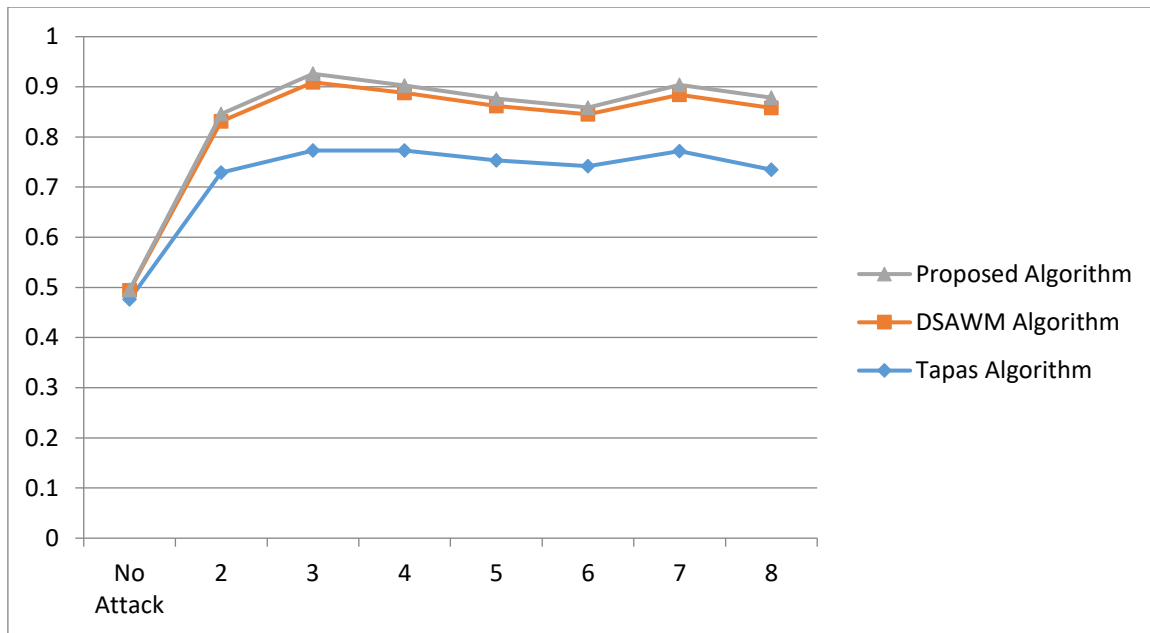
Table 5.2 Comparison between PSNR,MSE values (Scaling attack)

Sr no.	Scaling attack ON LENA	Tapas et al. algorithm		DSACM algorithm		Proposed System	
		PSNR	MSE	PSNR	MSE	PSNR	MSE
1.	NO ATTACK (256*256)	51.348	0.476	65.382	0.0188	86.25	.00012
2.	(256*254)	29.500	0.72957	28.029	0.102358	51.0229	0.0150
3.	(230*229)	29.244	0.77378	26.767	0.136866	50.889	0.0174
4.	(258*250)	29.245	0.77310	27.507	0.115422	51.0978	0.0149
5.	(257*253)	29.361	0.75328	27.723	0.109841	51.1215	0.0147
6.	(260*270)	29.215	0.74251	26.532	0.102532	51.2108	0.0138
7.	(200*215)	28.256	0.77256	27.263	0.112532	50.6844	0.0201
8.	(130*150)	27.262	0.73512	27.112	0.123512	50.6844	0.0201

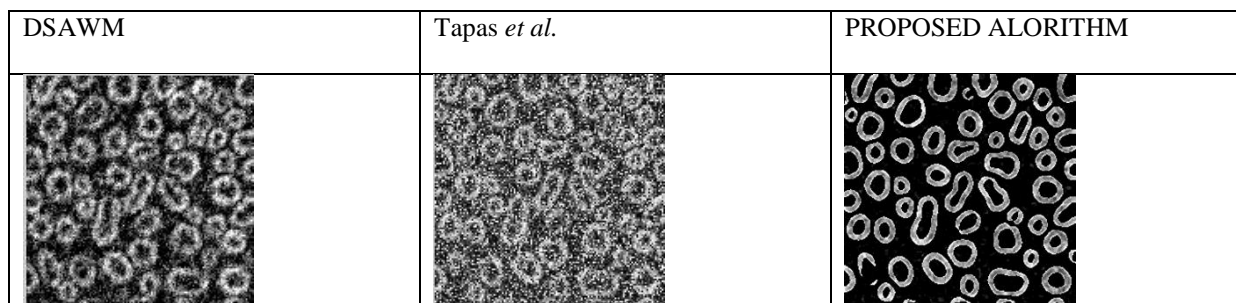
PSNR Comparison Graph



MSE Comparison Graph



A: shows scaling effect on both the algorithms visually.



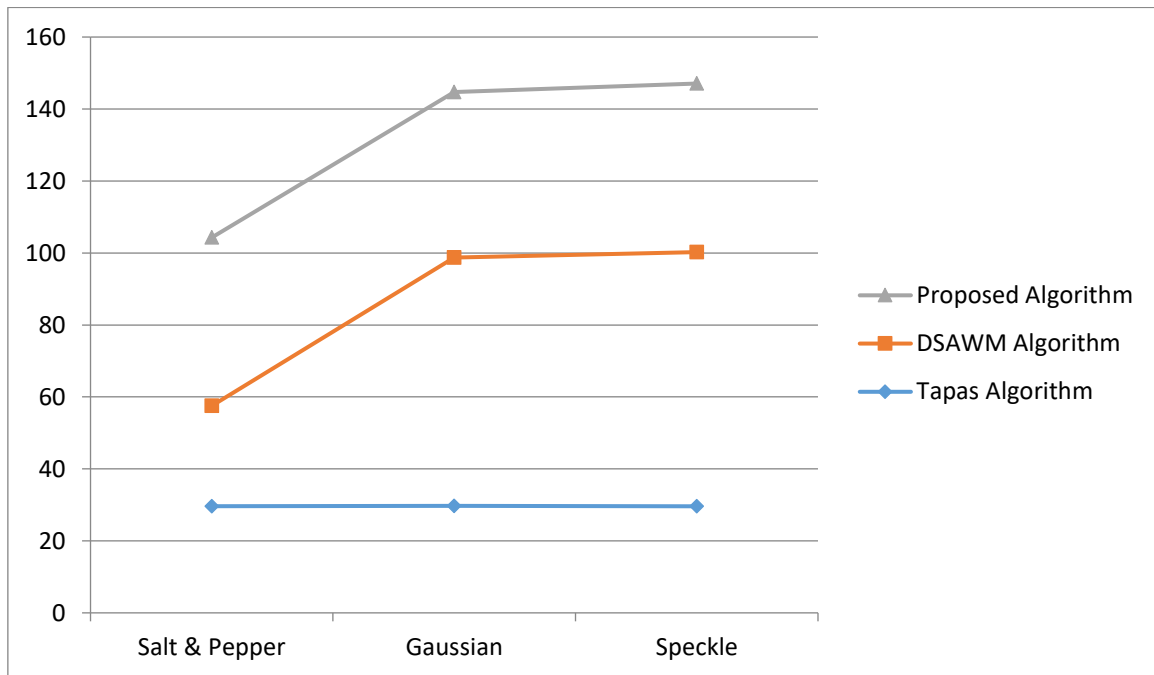
Noise Attack

NOISE: Watermarked image was subjected to various noise attacks such as salt & pepper, gaussian and speckle. Results in terms of performance parameters (PSNR, MSE)

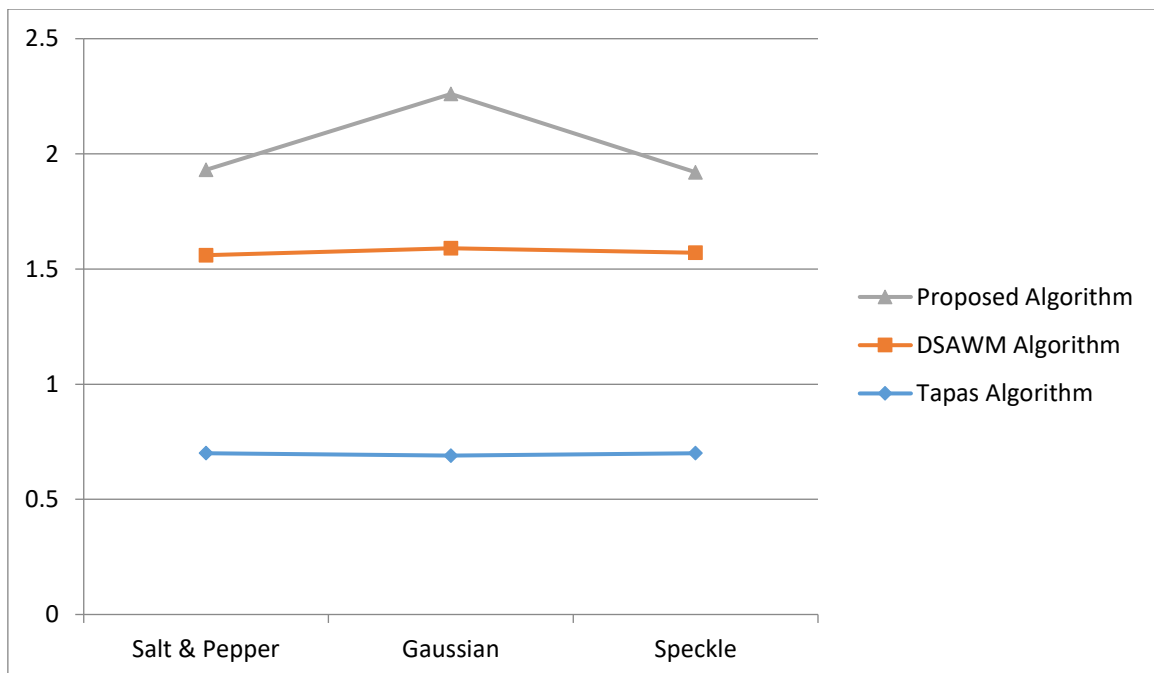
Table 5.3 Comparison between PSNR, MSE values (Noise Attack)

Sr no.	NOISE attack ON LENA	Tapas et al.		DSACM algorithm		Proposed System	
		PSNR	MSE	PSNR	MSE	PSNR	MSE
1.	SALT & PEPPER	29.632	70.766	27.879	0.860	46.7760	0.3720
2.	GAUSSIAN NOISE	29.739	69.042	28.645	0.906	45.9428	0.6776
3.	SPECKLE	29.642	70.6020	28.212	0.873	46.8427	0.3546

PSNR Comparison Graph



MSE Comparison Graph



6. CONCLUSION

Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing the multimedia data. Though a new algorithm has required to be implemented to overcome the difficulties and to assure copyright. In this research work a new approach for watermarking of digital images is to be implemented. The new approach will tested on various images. Here we have tested this system on 50 different images. In the proposed system a new technique is developed to watermark the images after encryption process. In addition to DES algorithm we use DWT and SVD to apply the watermark. Proposed system is also tested on various types of attacks on the watermarked images to check the robustness of the system.

7. FUTURE WORK

The upcoming era needs higher security enhancements in watermarking in which the various high security encoding techniques can be used as well as the techniques which significantly recover the watermark from watermarked image after combination of various attacks. Proposed system can also be extended to apply the watermark on video files.

REFERENCES

- [1] A. Ahmad, G. R. Sinha ,N.Kashyap (2014)“ 3-Level DWT Image Watermarking Against Frequency and Geometrical Attacks”I.J. Computer Network and Information Security, 12, pp. 58-63
- [2] A.Akter,M.A.Ullah(2014)“Digital Watermarking With A New Algorithm” International Journal of Research in Engineering and Technology, Volume: 03 Issue: 03 pp. 212-217
- [3] Aaqib Rashid(2016,"Digital Watermarking Applications and Techniques: A Brief Review",International Journal of Computer Applications Technology and Research Volume 5–Issue 3, 147-150
- [4] B.Singh, K.D.Sharma,L.S.Jatav (2014) “New Robust Watermarking Approach for Image Authentication ” IEEE third conference on consumer electronics pp. 285-288
- [5] B.Surekha ,G.N.Swamy (2013) “ Sensitive Digital Image Watermarking for Copyright Protection” International Journal of Network Security, Vol.15, No.2,pp.113-121
- [6] C.H.Chen, Y.L.Tang , W.S.Hseih(2014) “ An image authentication and recovery method using optimal selection of block types ”IEEE international symposium on multimedia ,pp. 151-154
- [7] Deepika Sardana, Ajit Singh(2016),"3-Level DWT Based Digital Image Watermarking ", International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1615-1619
- [8] G.Kaur ,K.Kaur(2013)“Implementing LSB on Image Watermarking Using Text and Image” International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 8, pp. 3130-3134
- [9] Gopika V Mane,G. G. Chiddarwar (2013),"Review Paper on Video Watermarking Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013
- [10]H. Kaur ,S. Kaur (2014) “Enhanced Watermarking Technique using Computational Wavelet and Cosine Transformation” International Journal of Science and Research (IJSR) Volume 3 Issue 8, pp.150-155
- [11]J.Jain , P.Johari (2014)“ Digital Image Watermarking Based on LSB for Gray Scale Image” International Journal of Computer Science and Network Security, VOL.14, No.6,pp. 108-112
- [12]J. Kaur,K.Kaur (2012)“ Digital Watermark: A Study” International Journal of Advanced Research in Computer Science and Software Engineering 2 (8), pp. 159-163
- [13]K. J. Giri, M.A. Peer,P. Nagabhushan (2014) “A Channel Wise Color Image Watermarking Scheme Based On Discrete Wavelet Transformation” International Conference on Computing for Sustainable Global Development , pp. 758-762
- [14]K.R. Reddy, S.T. Mahaboob, S. K. Chandra, T.S.M.Basha (2014) “Secured Data Transmission Using Wavelet Based Steganography and cryptography” Int. Journal of Engineering Research and Applications , Vol. 4, Issue 2, pp.45-50
- [15]Kapil Kumar Singh, Sandhya Tarar (2019),"Watermarking Techniques based on DCT and SVD using PSO", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-3, January 2019
- [16]K. Rameshbabu, P.Prasannakumara, K.E.Balachandrudu(2013) “Text Watermarking Using Combined Image & Text” International Journal of Engineering Research & Technology Vol. 2 Issue 12,pp. 3812-3818
- [17]L.Dong, R.Wang (2014) “ A blind digital watermarking algorithm based on DWT ” Journal of Chemical and Pharmaceutical Research, 6(3), pp. 78-89
- [18]Lalit Kumar Saini, Vishal Shrivastava (2014),"A Survey of Digital Watermarking Techniques and its Application", International Journal of Computer Science Trends and Technology (IJCTST) – Volume 2 Issue 3, May-Jun 2014
- [19]M.Craig , D.Kapgate(2014)“Effective Copyright Protection of Digital Products by Embedding Watermarking” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, pp. 859-864
- [20]Mohan Durvey, DevshriSatyarthi(2014),"A Review Paper on Digital Watermarking", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 3, Issue 4, July-August 2014

- [21] M.Mundher, D.Muhamad, A.Rehman, T.Saba , F.Kausar (2014) “Digital Watermarking for Images Security using Discrete Slantlet Transform” Applied Mathematics & Information Sciences An International Journal 8, No. 6, pp. 2823-2830.