International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 216-222
Published Online August 2020 in IJEAST (http://www.ijeast.com)

SECURITY AND COPYRIGHT PROTECTION TECHNIQUE FOR DIGITAL IMAGE

Ms. Manjula B
M Tech, 4th SEM, Department of CSE,
J.N.N College of Engineering,
Shivamogga, Karnataka, India

Mr. Hiriyanna G S
Assistant Professor, Department of CSE,
J.N.N College of Engineering,
Shivamogga, Karnataka, India

Abstract— **The information's are transformed from transference spot to the destination spot through the digital communication. For maintaining the quality of images and transferring the information's, there are many techniques. And also the information's may be in different forms like audio, images, graphics, messages, animated forms or texts. While transferring the information from one medium to another medium there is need for security and copyright protection. Here, for the experiment 2 dimensional images are used. To provide security and copyright protections services there many different types of techniques. The Advanced Encryption Standard (AES) techniques is used to provide the security services and the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) is combined watermarking technique is used for copyright protection services. To provide security, authenticity, copyright protection to the images for the different attacks like salt and pepper noise, speckle noise, Gaussian noise and poisson noises, the combined digital image watermarking and AES technique is used.**

Keywords— **DWT, DCT, AES, Encryption, Watermarking, Watermark, Copyright Protection, Attacks**

I. INTRODUCTION

Data communications helps us to transmit the information's from one station to another station. To maintain the standard and to transfer the information's the interactive media is required. The information's are of different kinds like graphic, photos, audio's, videos, texts, messages or animated forms. While transferring the information's, the protection from copyright and security is provided to the information's and it is very important for secure transmission [3, 4, 5]. Here, for this experiment, using the 2 dimensional images. Many different kinds of algorithm and techniques, methods to provide the protection from copyright and security, but here we are using the DCT and DWT to provide the protection from copyright and to provide the security we are using the Advanced Encryption Standard (AES) technique and in this the key used for Advance encryption is 256 bits. The watermarking of images and also AES techniques are combined together to provide the security and protection from copyright against the different kinds of attacks [14, 5].

The images are most extensively used for many activities. So, it is very important to provide the protection from unauthorized users. To hide the information's from the public, encryption method plays a major role by hiding the important information's and makes the information's unreadable. So, that no hackers or eavesdropper, including server administrator and others, who have access during the transmission can also can't access the information's other than the original owner. So, ability to get an original images and also creating the strong encryption, such that the information's are not hacked or modified. If the encryption time is smaller, the images are transferred fast and original images are obtained after decrypting the images.

The rest of the paper is organized as follows. Related works are explained in section II. Techniques used for watermarking and encryption are explained in section III. Proposed method and working of proposed method are explained in section IV and V respectively. Experimental results and analysis are presented in section VI. Conclusion are given in section VII. Finally the references are in VIII.

II. RELATED WORK

There is the necessity for the information security and copyright protection, because of the rapid development in the interactive media. Here, the technique used which makes the images invisible or hidden and other than owner doesn't know the information is hidden inside one another (Raymond et al 2007 in their work). So, this hiding technique is called as image watermarking. The image watermarking is classified into two types. In this main aim is to provide the customer rights and also to protect the ownership of the images [1]. The only method that was guaranteed for the user identity is the biometrics. By using the cancelable biometric information's, the watermark is added and it helps to the information security and privacy complaint identity verifications [2].

The Generalized Singular Value Decomposition (GSVD) is the new technique which is used for the watermarking in this experiment. By using the watermarking the elements are placed on the original images, and also used to control many factors like impartibility and robustness [3]. Implanting the watermarks, first copyright insertion takes place then authenticity insertion is done, finally to get the original image, we have to detect the watermarks likewise detecting copyright and authentication [4].

III. DWT AND DCT WATERMARKING AND AES ENCRYPTION

A. Working of DWT

Based on the location and frequency, the discrete wavelet holds the information's. Using these things the images are separated into 4 parts without overlapping. Each parts are approximated, they are LL_1, HL_1 the horizontal part, LH_1 the vertical part and HH_1 the diagonal part of the images. The '1' indicates that it is a 1 level DWT is applied to the images as represented in the figure 1.

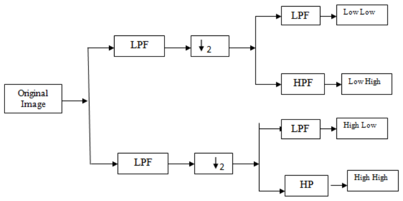


Figure 1 Dividing Images into 4 parts by applying DWT

The signals are decomposed by using Discrete Wavelet and form the basic functions. The signals formed are known as the wavelets. The wavelet functions are formed from their parent wavelet functions [5,11].

B. Working of DCT

The discrete cosine is the sum of the order of the limited cosine functions that are oscillating at the non identical frequencies and the amplitude is varying. The discrete cosine part is as shown in the figure 2.

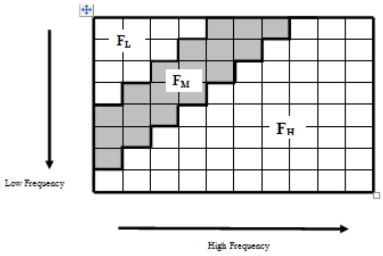


Figure 2 Watermark used to Embed in DCT Define Region

C. Combined DWT & DCT Watermarking

To guard the images from issues and also the unlawful modifications of the information's, to protect from these the watermarking technique is used. The DWT of watermarking is most frequently used technique than other techniques. It is because this technique is like human sensual structure which is having the features like wild spreading, spatial flooding and spread iteratively. This technique explains the powerful and the unnoticeable algorithms called the DWT and DCT together. Watermarks are applied to the images using the two techniques that is cosine and wavelet transforms to hide the content to provide the strong protection from the copyrights and hacking [5,11,15].

D. Advanced Encryption Standard Encryption of Images

Various techniques are used to secure the digital images, such as encryption, decryption, stenography and watermarking, to achieve the security goals that confidentiality, integrity and availability. Here in this experiment, using the AES encryption because it is better and it is numerically structured and its principle strength of encryption of range of the key [14].

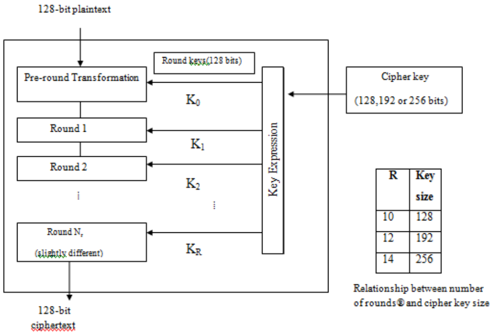


Figure 3 the Schematic of AES Encryption

The structure of AES process is shown in the figure 3. In encryption, the information's are converted into cryptic form called as cipher text. And decryption converts back into original form is called plain text.

IV. PROPOSED METHOD

The proposed method is split into three parts. The embedding part is the first phase; on the original image the logo watermarked image is added. Next phase is the second phase that is called attack part where the different kinds of attacks and noises are added to the watermarked combined DCT and DWT and encrypted image, the encryption algorithm here used is the Advanced Encryption Standard. The next phase is the third part that is called the extraction part where the logo watermarked image is extracted from the AES decryption and DCT and DWT watermarked image.

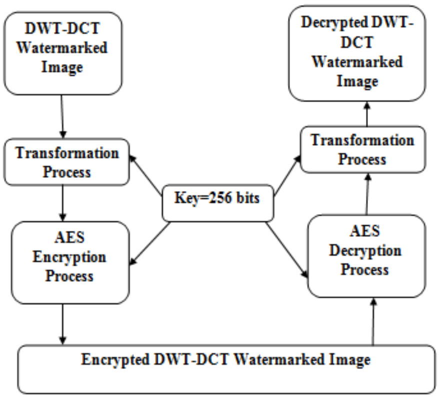


Figure 4 Block diagram of complete process

V. WORKING OF PROPOSED METHOD

A. Flow Chart of Insertion of Watermark and Encryption Process

- Choose 2Dimentional image as input.
- The watermarked image is selected and the selected image is colored then it is converted into gray scale image.
- After converting the image into the gray scale, on that cover image level one discrete wavelet transform operation is carried out and as a result the image is divided into 4 bands that are $LL_{1,}$ $LH_{1,}$ HL_1 and $HH_{1,}$ without overlapping.
- The LL_1 band of the image is choose from the four bands of discrete wavelet transform, on that LL_1 discrete cosine transform is applied.
- Then the chosen watermarked logo gray scale image is then transformed into the vectors sequences that are sequence of zeroes and ones [11,15]
- Then the PN_Sequence is generated, where each PN_Sequence are dissimilar. The PN_Sequence bit 1 is used to insert the watermark insertion and the PN_Sequence bit 0 is used to embed the watermark [11,15].
- The S_0 & S_1 are the two different types of PN_Sequences that are used to insert the logo image watermarking by making use of scaling factor α, that is in mid frequency element of discrete cosine transform altered discrete wavelet transform estimated bands.
- The following equations are used in inserting, when the watermarked logo bit 0 then;
  $IW = [(\alpha) \times S\_1)] + I$
  Or else;
  $IW = [(\alpha) \times S\_0] + I$
- The mid frequency elements are updated properly, the elements are coefficients, for inserting bits inverse of discrete cosine transform is applied.
- On the updated bands of the image apply the inverse of discrete wavelet transform, then we will get the combined discrete wavelet transform and discrete cosine transform watermarked image.
- On the combine discrete wavelet and discrete cosine transformed watermarked image, the advanced encryption standard technique is applied using the key length of 256 bit.
- Ultimately, we get the combined discrete wavelet transform and discrete cosine transformed watermarked and advanced encryption standard encrypted technique applied image.

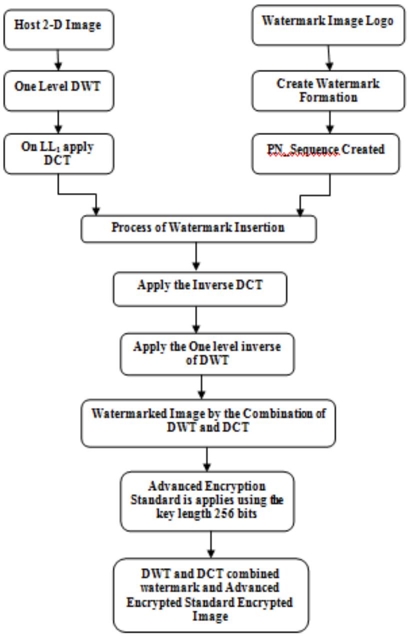

Host 2-D Image
One Level DWT
On LL1 apply DCT
Watermark Image Logo
Create Watermark Formation
PN_Sequence Created
Process of Watermark Insertion
Apply the Inverse DCT
Apply the One level inverse of DWT
Watermarked Image by the Combination of DWT and DCT
Advanced Encryption Standard is applies using the key length 256 bits
DWT and DCT combined watermark and Advanced Encrypted Standard Encrypted Image

Figure 5 Working of Combined DWT-DCT Watermark Insertion & 256 bits key AES Encryption Process

B. Flow Chart of Decryption Process

- Extraction of images from the DWT and DCT watermarking and advanced encryption standard decryption.
- Based on the figure 6, the images are extracted from the combined DWT and DCT watermarking and Advanced Encryption Standard technique using 256 bit key length technique.
- Choose image which is watermarked and encrypted by using combined DWT and DCT watermark technique and Advanced Encryption Standard technique.
- By using the key of length two fifty six the decryption of advanced encryption standard is carried to obtain the combine discrete wavelet transformed and discrete cosine transformed watermarked images.
- Then, on the decrypted watermarked image, discrete wavelet transform is putted in. So, the images are separated as 4 bands (LL_1, LH_1, HH_1, HL_1) without overlapping that is applying discrete wavelet transform.

- In general two PN_Sequences are generated; they are S_0 & S_1 over the images that are differing over each other's [4].

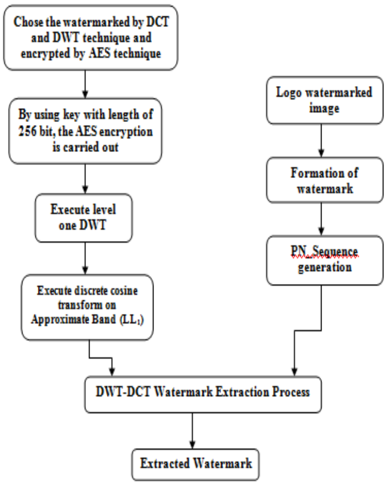

Chose the watermarked by DCT and DWT technique and encrypted by AES technique
By using key with length of 256 bit, the AES encryption is carried out
Execute level one DWT
Execute discrete cosine transform on Approximate Band (LL1)
Logo watermarked image
Formation of watermark
PN_Sequence generation
DWT-DCT Watermark Extraction Process
Extracted Watermark

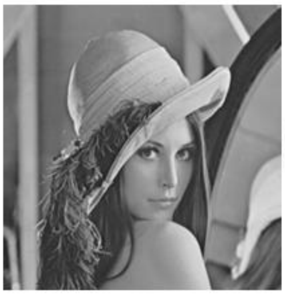
Figure 6 Extraction from Combined Discrete Wavelet and Discrete Cosine Transform and the Decryption Process for AES Encrypted Image

- The correlation is checked for the extraction bit 1 is used, if and only if correlation of S_1 is bigger than the S_0 or else bit 0 is considered as the watermark extracted bit.
- The image which is extracted from the similar characters and the original source image are obtained after repairing and recovering of the images as the above processes.

VI. EXPERIMENTAL RESULTS AND ANALYSIS

A. Inputs of the Experiment

Here, take the first input i.e., figure 7 as the cover image which is visible to all, then taking the figure 8 as the secrete image that is logo picture.



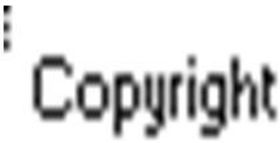


Figure 7 Cover Picture as Input

Figure 8 Secrete Image

B. Outputs of the experiment

The output screenshot of the experiment in figure 9 explains that without adding any external noise but there is a default noises added and got the secrete image and also we can recovered the cover image.

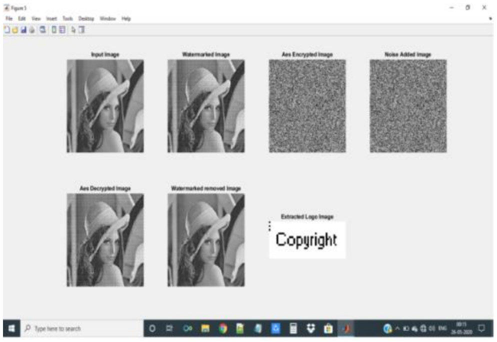


Figure 9 Output of Recovering Secret Image without Applying Any Noises

The output screenshot of the experiment in figure 10, when the external noises are added externally, here the external noise is Gaussian noise, where we can recover the secrete image as well as we can recognize the cover image also.

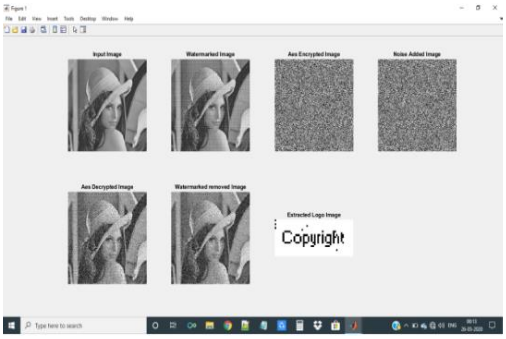


Figure 10 Output of Recovering Secrete Image with Gaussian Noise Is Applied

The output screenshot of the experiment in figure 11, when the external noises are added externally, here the external noise is poisson noise, where we can recover the secrete images as well as we can recognize the cover image

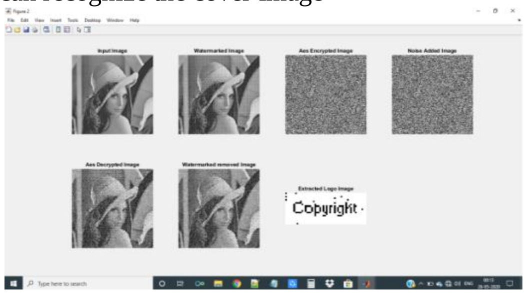


Figure 11 Output of Recovering Secrete Image with Poisson Noise Applied

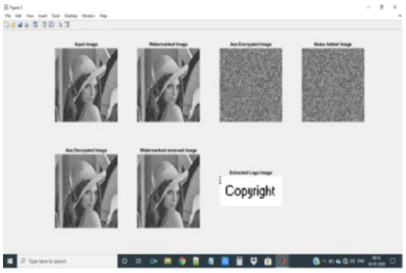


Figure 12 Output of Recovering Secrete Image with Salt and Pepper Noise Applied

The output screenshot of the experiment in figure12, the external noises are added externally, here the external noise is salt and pepper noise, where we can recover the secrete image as well as we can recognize the cover image.

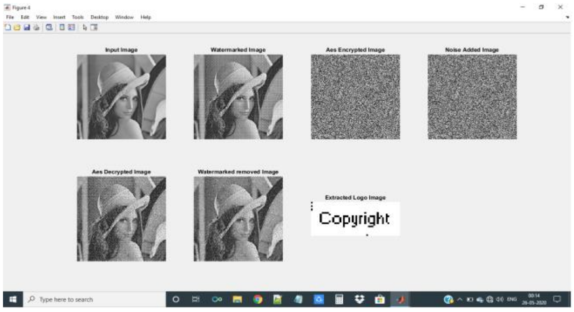


Figure 13 Output of Recovering Secrete Image with Speckle Noise Applied

The output screenshot of the experiment in figure 13, when the external noises are added externally, here the external noise is speckle noise, where we recover the secrete image as well as we can recognize the cover image also.

C. Analysis of Results using Graph

The overall process of the experiment is analyzed using the graph by recording the values in the table according to the values recorded in the table the graph is plotted to analyze the results of the experiment.

Different Types of Attacks	Watermark Embedding Time(Sec)	AES Encryption Time(Sec)	AES Decryption Time(Sec)	Removing Watermarking Time(Sec)	Returning Logo Image Time(Sec)
Gaussian Noise	0.1969	3.974	3.996	0.1129	0.1415
Poisson Noise	0.1969	3.974	3.771	0.1129	0.1415
Salt and Pepper Noise	0.1969	3.974	3.892	0.1129	0.1584
Speckle Noise	0.1969	3.974	4.177	0.1129	0.1415
Normal (Without Any Attack)	0.1969	3.974	3.817	0.1129	0.1415

Table 1 Execution Time Taken To Complete the Process along the Scaling Factor

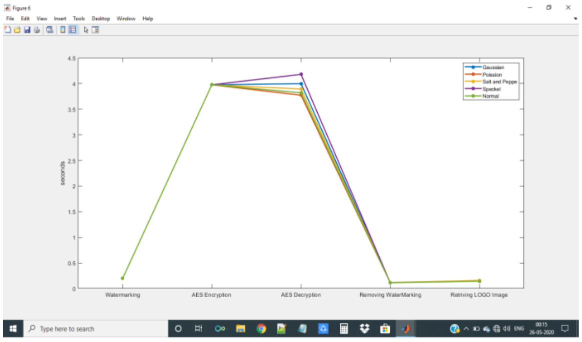


Figure 14 Graphs to Execution Time Taken to Complete the Process along the Scaling Factor

In table 1 the values are recorded for the time required to execute each processes of the experiment against different noises applied and also without applying noises, and getting the same values with little changes .And the figure 14 shows the graphical representation of the time taken to execute each processes against different noises applied and also without applying any noises. So, time taken to execute the results is in few seconds for all the process.

Different Types of Attacks	Transmitted vs. Received Cover Image	Encrypted vs. Decrypted Stego Image	Transmitted vs. Received Secrete Image
Gaussian Noise	19.62	8.98	71.14
Poisson Noise	18.37	8.909	67.34
Salt and Pepper Noise	29.35	9.2777	100
Speckle Noise	20.68	9.057	78
Normal (Without Any Attack)	68.27	9.297	100

Table 2 against Different Types of Attacks, the PSNR Values Are Recorded

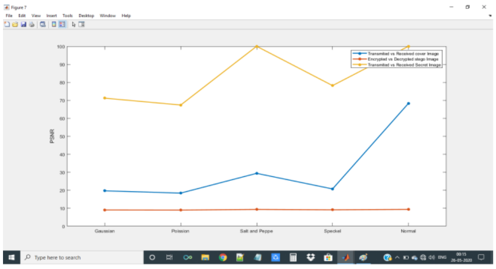


Figure 15 the Graphical Representation of the Values of PSNR against the Different Types of Attacks

As shown in the above table 2 the values of PSNR are calculated to the transmitted vs. received cover image, encrypted vs. decrypted stego image and transmitted vs. received secrete image against the different noises and also without applying any noises. Here, getting the high PSNR values for the transmitted and received secrete image as shown in the table. As the values of the PSNR are high we are getting the better quality of images. And the figure 15 which is the represents, the PSNR value calculated against different noises and also without applying any noises.

Different Types of Attacks	Transmitted vs Received Cover Image	Encrypted vs Decrypted Stego Image	Transmitted vs Received Secrete Image
Gaussian Noise	14.14	3.541	22.5
Poisson Noise	12.94	3.53	18.68
Salt and Pepper Noise	23.7	3.679	100
Speckle Noise	15.15	3.578	29.51
Normal (Without Any Attack)	62.62	3.691	100

Table 3 against Different Types of Attacks, the SNR Values Are Recorded

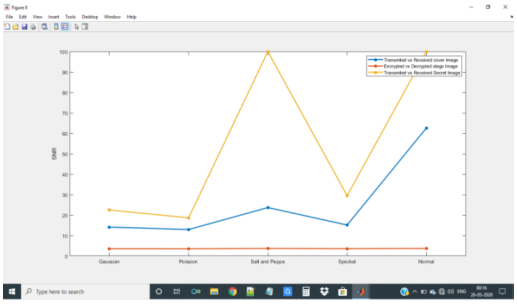


Figure 16 the Graphical Representation of the Values of SNR against the Different Types of Attacks

In table 3 the SNR values are calculated for the transmitted vs. received cover image, encrypted vs. decrypted stego image and transmitted vs. received secrete image against the different noises and also without applying any noises. Here, getting the high SNR values for the transmitted and received secrete image as shown in the table. As the values of the SNR are high we are getting the better quality of images. And the representation of values of SNR values against the different kinds of attacks is shown in the figure 16.

Different Types of Attacks	Transmitted vs Received Cover Image	Encrypted vs Decrypted Stego Image	Transmitted vs Received Secrete Image
Gaussian Noise	709.1	8224	0.005
Poisson Noise	947.2	8360	0.012
Salt and Pepper Noise	75.61	7680	0
Speckle Noise	556	8079	0.001
Normal (Without Any Attack)	0	7644	0

Table 4 against the Different Types of Attacks, the MSE Values Are Recorded

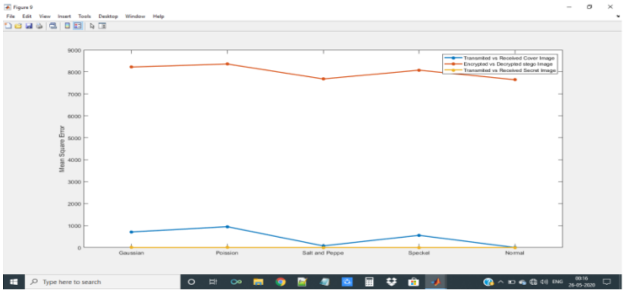


Figure 17 the Graphical Representation of MSE Values against the Different Types of Attacks

In table 4 the MSE values are calculated for the transmitted vs. received cover image, encrypted vs. decrypted stego image and transmitted vs. received secrete image against the different noises and also without applying any noises. Here, getting the MSE values which is near to zero or zero values for the transmitted and received secrete image as shown in the table. As the values of the MSE are near to zero or zero we are getting the better quality of images. And the MSE values are calculated against the different types of noises and also without applying noises are represented in the figure 17.

VII. CONCLUSION

The experiment purpose is to provide the security and copyright protection for the input and output images. Here, applied Combined DWT and DCT watermarking and AES encryption techniques are used for the purpose of security and copyright protection. And getting better PSNR and SNR values after applying the different types of noises and secrete logo image also obtained with lesser MSE values, so getting better quality with secured secrete image is extracted and also we can recognize the cover image. In this experiment, without adding noises and also when the salt and pepper noises are added, we are getting more accurate and better quality of secrete images.

VIII. REFERENCE

[1] Raymond B. Wolfgang and Edward J, (2007), “A Watermark for digital images”, Computer Vision and Image Processing Laboratory School of Electrical Engineering Purdue University West Lafayette, Indiana, 4707-1285 USA.

[2] Morgan Barbier, Jean-Marie Le Bars, and Christophe Rosenberger, (2015), “Image Watermarking With Biometric Data for Copyright Protection” ENSICAEN-UNICAEN-CNRS, GREYC, F-14032 Caen, France.

[3] Bambang Harjito, (2016), “False-Positive-Free GSVD-Based Image Watermarking for Copyright Protection”,

Department of Informatics University as Sebelas Maret, Surakarta, Indonesia. International Symposium on Electronics and Smart Devices (ISESD).

[4] Jen-Sheng Tsai, Win-Bin Huang, Chao Lieh Chen, Yau-Hwang Kuo, (2007), "A Feature-Based Digital Image Watermarking For Copyright Protection And Content Authentication", Dept. of computing and knowledge Engineering National Cheng Kung University, Taiwan, R.O.C.

[5] Sudhanshu Suhas Gonge and Ashok A Ghatol, (2017), "An Enhancement in Security and Copyright Protection Technique Used For Digital Still Image", International Conference on National Technologies in the Engineering (ICNTE-2017).

[6] Mal MalhdiMosleh, saeesetayeshi, mohammadMosleh, Presenting a Novel, (2011), "Audio Watermarking based on Discrete Wavlet Transform", International journal of computer and electrical engineering, vol 3, no 4, 2011, pp 587-590

[7] P. Bassia and I. Pitas, (2001), "Robust audio watermarking within the time domain", IEEE transactions on Multimedia, Vol. 3, Issue: 2, 2001, pp. 232-241.

[8] C.M.juli Janardhanan, C. Satish Kumar, (2013), "Performance Analysis of Discrete Wavelet Transform based Audio Watermarking on Indian Classical Songs", vol.33, 2013 international journal of computer application, vol.33, 2013, pp-0975-8887.

[9] cai Yong-mei, guo Wen-qiang, ding Hai-yang, (2013), "An Audio Blind Watermarking Scheme Based on DWT-SVD", Journal of Software ,Vol 8,No.7,July 2013.

[10] Musrrat AliChang Wook Ahn, (2014), "An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain, Signal Processing", vol.94,2014,pp-545–556.

[11] Sudhanshu Suhas Gonge, Ashok A Ghatol, (2016), "A Hybrid Intelligent Security Technique used for Digital Still Image", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 856 – 865,21-24 Sept. 2016, Jaipur, India.

[12] William Stallings, (2005), "Cryptography and Network Security Principles and Practices", Fourth Edition.

[13] W.Stallings and NJ: Prentice Hall, (2003) "Cryptography and Network Security",. 2003.

[14] Praveen.H.L, H.S Jayaramu, M.Z.Kurian, (2012), "Satellite Image Encryption Using AES" International Journal of computing and EE (IJCSEE) ISSN No. 2315-4209, Vol-1, Iss-2, 2012.

[15] Sudhanshu Suhas Gonge, Ashok A.Ghatol, (2014), "Combination of Encryption and Digital Watermarking Techniques used for Security and Copyright Protection of Still Image." IEEE International Conference on Recent Advanced and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.